TRUCOS WINDOWS: OCULTAR, ENCRIPTAR Y PROTEGER CARPETAS IMPORTANTES



LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA

BANDA ANCHA
VÍDEOS EN STREAMING

INTERNET
LOS ENTRESIJOS DEL CIBERCRIMEN

PROGRAMACIÓN
FLICKR3DCUBE, DESARROLLO DE UN GADGET

VOIP
RIESGOS EN LAS COMUNICAIONES VOIP

PISHING

Alerta con los ladrones de identidad

Y ADEMÁS...
Implantación de un servidor Subversion

CURSO DE JAVA ÚTIL
jWadalPasswd (V)

RETROINFORMÁTICA
Discos y memorias encriptadas



Directora: Montse Fernández
(montsef@mcediciones.com)

Colaboradores: Ferran Caldés, Toñi Herrero, Sara Rojas, Ana Rueda, Francisco Javier Palazón, Susana Velasco, Regina de Miguel, Laura Pajuelo, Jorge García López.

Fotógrafos: Sebastián Romero.

Maquetación: Domingo Melero.

Publicidad
Directora comercial: Carmen Ruiz
(carmen.ruiz@mcediciones.com)
Menchu de la Peña
(mdelapena@mcediciones.com),
Orense, 11. 28020 Madrid
Tel: 91 417 04 83 . Fax: 91 417 05 33

Suscripciones: Fernando García (fgarcia@mcediciones.com)
Tel: 91 417 04 83

Edita:



Editora: Susana Cadena
Gerente: Jordi Fuertes
Redacción, Administración y Departamento de Publicidad
Paseo San Gervasio, 16-20.
08022 Barcelona
Tel: 93 254 12 50 - Fax: 93 254 12 63

Oficina de Madrid
C/ Orense, 11 bajos
2820 Madrid
Tel. 91 417 04 83
Fax: 91 417 04 84

Distribución:
Coedis S.A. Avda. de Barcelona, 225 - Molins de Rei, Barcelona
Coedis Madrid: Alcorcón,9
Pol Ind. Las Fronteras-Torrejón de Ardoz, Madrid

Fotomecánica: MC Ediciones, S.A.
Paseo San Gervasio, 16-20.
08022 Barcelona

Impresión: Litografía Rosés

Tel. 93 633 37 37

Precio de este ejemplar: PVP 4,95 € (IVA incluido)
Precio para Canarias, Ceuta y Melilla:
4,95 € (incluye transporte)
Depósito legal: MA-1049-97 / nº147

FIREFOX CUMPLE CINCO AÑOS

La herramienta más universal es hoy el navegador web, pero a pesar de su papel estratégico para la humanidad, este utensilio estuvo a punto de ser un monopolio de facto. Hoy este peligro por fortuna ha desaparecido, especialmente gracias a Firefox. El navegador gratuito y de código libre de la Fundación Mozilla cumple el día 9 de este mes de noviembre sus primeros cinco años de existencia. Firefox, no ha parado de crecer en cuota de mercado, y se ha convertido hoy en un espectacular centro de innovación y de proyectos complementarios. Su éxito nos ayuda a olvidar sus complejos antecedentes, desde hundimiento del navegador Netscape a manos de Internet Explorer de Microsoft, el papel de AOL y su desinterés creciente, hasta su abandono total y el despido del equipo de desarrolladores... Lo cierto es que su historia no ha sido fácil ni cómoda, y que pocos creían en el futuro de aquel proyecto. Pero Firefox es hoy un navegador multiplataforma, disponible en 75 idiomas, rápido, cómodo y seguro y cuenta con múltiples funcionalidades pioneras. Su empuje ha obligado a renovarse a fondo a sus rivales (basta comparar las funciones de las versiones anteriores de IE con las de IE 8, por ejemplo), de modo que al final, el proyecto Firefox ha beneficiado tanto a sus usuarios como a los de otros navegadores web. Un vez más se demuestra que tener la posibilidad de elegir suele ser una situación más favorable que la imposibilidad de hacerlo. Una vez más se cumple que un escenario de competencia es la garantía de la innovación tecnológica. Así pues, ¡feliz cumpleaños!

[SUMARIO número 147]



Malas prácticas en la gestión de usuarios privilegiados

Las malas prácticas en la gestión de usuarios privilegiados representan una amenaza para la seguridad de las empresas europeas. Esta es la principal conclusión del estudio titulado *Privileged User Management_It's Time to Take Control,* elaborado por la firma Quocirca para CA. Los usuarios privilegiados suelen ser los administradores de la red o de TI responsables del mantenimiento y disponibilidad de los sistemas, o también los administradores de sistemas operativos, aplicaciones de negocios, seguridad y bases de datos. Por lo general, a éstos se les conceden unos derechos de acceso dentro de la infraestructura TI de las empresas que son significativamente mayores que los derechos de la mayoría de usuarios de TI. El estudio destaca que el 41% de los encuestados europeos (40% en España) que señalan haber implementado el estándar ISO27001 aún mantienen algunas prácticas no conformes con la normativa como el compartir cuentas de usuarios privilegiados. Esto se suma a otra mala práctica como es el uso de los nombres de usuario y contraseñas por defecto para las cuentas privilegiadas. Si se consideran sólo aquellos que han implementado el estándar ISO27001 y tienen la certificación de un auditor externo, esta cifra continúa manteniéndose alta, con un 36%. A pesar de estos riesgos, la investigación revela que el control y la monitorización de la actividad de los usuarios privilegiados no ocupan un lugar destacado en la agenda de los responsables de TI. Además existe un exceso de confianza en la capacidad de gestionar los usuarios privilegiados. Los encuestados también están relativamente seguros de poder pasar una auditoria de cumplimiento y se preocupan más de temas como pérdidas de datos o de la violación de la propiedad intelectual.

Nuevo dispositivo de seguridad



WatchGuard Technologies presenta Watchguard XTM 8 Series, un nuevo dispositivo de seguridad multifunción que proporciona un rendimiento sin precedentes y protección contra la próxima generación de amenazas de datos, de aplicaciones y de red.

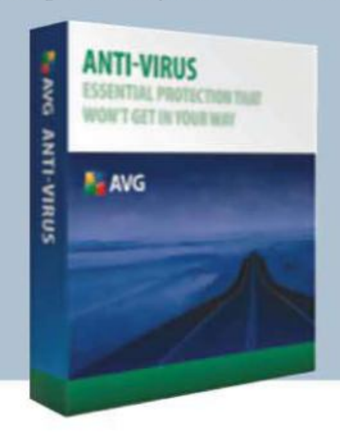
WatchGuard XTM 8 Series ofrece un rendimiento del cortafuegos de 5 Gbps, lo que lo convierte en un dispositivo ideal para las exigencias de las redes de entre 1.000 y 5.000 usuarios. Con completas funcionalidades de seguridad activadas, es más rápido que la velocidad de línea alcanzando un rendimiento de 1,2 Gbps, lo que supone un gran avance para los dispositivos de gestión unificada de amenazas proporcionando altos niveles de seguridad sin comprometer el rendimiento de la red. Aprovechando la tecnología cortafuegos de defensa en profundidad de WatchGuard, que incluye Stateful Packet Inspection, inspección de paquetes en profundidad y la exclusiva tecnología proxy de WatchGuard, el nuevo dispostivo XTM 8 Series incorpora las últimas tecnologías de seguridad para proteger las redes corporativas.

IREO distribuirá las soluciones de Deepnet

De esta forma, la plataforma Deepnet Unified Authentication llega a España de la mano de IREO, quien la distribuirá en exclusiva. Deepnet Unified Authentication es una de las herramientas de autenticación más versátiles del mercado. En concreto, consiste en una única solución de fácil instalación que permite la autenticación en múltiples escenarios. Ofrece compatibilidad out-of- the-box con una amplia variedad de aplicaciones y sistemas, utilizando a su vez los más diversos métodos de autenticación.

AVG 9.0

Con esta nueva suite de seguridad, AVG impulsa mejoras significativas en la velocidad y en los niveles de protección. Las nuevas tecnologías aplicadas en los productos AVG garantizan la seguridad del usuario en cualquier actividad realizada en la sociedad online de hoy. La nueva versión está dotada de un motor de análisis de nuevas tecnologías de rastreo lo que optimiza el análisis es una de nuestras prioridades en los productos AVG 9.0, Marcando los archivos como seguro o potencialmente peligrosos, durante el primer análisis, se prioriza el análisis sobre los archivos marcados como potencialmente peligrosos. Dicho de otro modo AVG analiza primero la estructura del archivo para buscar cambios, en caso de haberlos, analiza el archivo. Acción que resulta en un ahorro de un 50% en el tiempo de análisis frente a los antivirus habituales. Además de proteger analizando los archivos infectados de código malicioso. La optimización de AVG 9.0 también favorece la rapidez de inicio de sistema así como el uso de memoria reduciendo el consumo de memoria e incrementando la velocidad de inicio en un 15%. La integración, en AVG 9.0, de los módulos Protección Residente, Firewall y Identity Protection permitiendo a los diferentes módulos compartir la información sobre malware entre ellos detectando y eliminado rápida y eficazmente todo tipo de malware, rootkits y ataques de robo de identidad. Además, AVG 9.0 aporta una mejor detección de phishing gracias al perfeccionamiento de LinkScanner que detecta en la mitad de tiempo y de manera más efectiva si un sitio web está siendo atacado por phishing u otro tipo de ataque online que pueda comprometer el equipo del usuario. Las soluciones AVG 9.0 están basadas en la comodidad del cliente sin descuidar su protección, incluso el proceso de instalación se ha acortado un 50% evitando que el usuario tenga que pasar por muchos de diálogos antes de poder instalar AVG.



El nuevo servicio Whois Privado de Piensa Solutions garantiza la privacidad

Piensa Solutions ha lanzado el nuevo servicio Whois Privado para los clientes que tengan registrado un dominio y desean reforzar su privacidad en la Red. Este servicio cumple con la normativa de registro de ICANN, la entidad reguladora de Internet, y protege los datos personales del titular del dominio, mediante la publicación de datos genéricos de Piensa Solutions.

En el registro de cada dominio, ICANN exige que el titular facilite sus datos de contacto (nombre, dirección postal, correo electrónico, teléfono...). Esta información se recoge en la base de datos Whois, accesible a través de la Red para los internautas de todo el mundo. Con el servicio Whois Privado, los datos de contacto del titular del dominio se sustituyen por información genérica de Piensa Solutions y una cuenta de correo electrónico aleatoria, redirigida a la del titular, que se modifica periódicamente. Este servicio cumple con las principales recomendaciones de los expertos en seguridad informática, que aconsejan no publicar datos personales en Internet. De este modo, se protegen los datos de contacto del titular de un dominio ante spammers y otros delincuentes que utilizan esta información para cometer prácticas ilegales, como el envío de correo publicitario no solicitado o la usurpación de identidad (phishing).

EL servicio Whois Privado tiene un coste de 3,95 euros al año para todas las extensiones de Internet (.com, .net, .org, .es, .cat...).



Seguridad para Mac en entornos empresariales

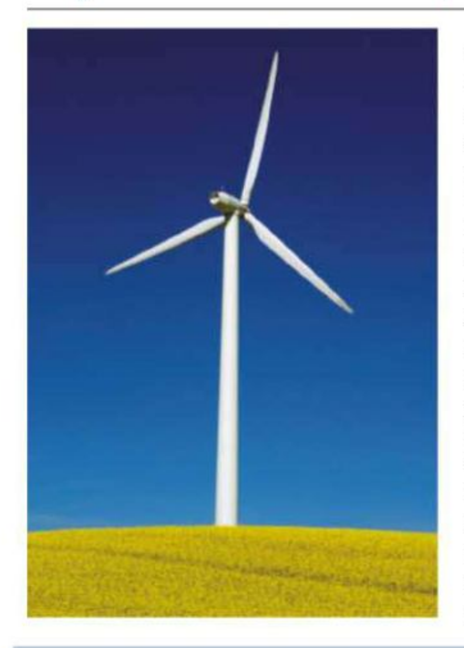
Trend Micro está ampliando su protección para endpoints a aquellas empresas que tratan de hacer compatibles la seguridad tanto para plataformas Windows como para Mac en sus redes corporativas. Trend Micro Security para Mac 1.5 está diseñado para proteger a los usuarios empresariales de Mac contra los ataques de virus, spyware, amenazas combinadas y ataques web a plataformas independientes. Se integra con Trend Micro OfficeScan Cliente/Server, que ha demostrado su eficacia a la hora de proteger millones de puestos de trabajo durante más de una década. La arquitectura plug-in extensible de OfficeScan permite a Trend Micro ofrecer a los clientes empresariales –muchos de los cuales están incorporando la plataforma Mac a sus redes corporativas- una mejor gestión de los sobremesa, portátiles y servidores Mac a través de la misma consola web que gestiona los clientes y servidores Windows. La solución incluye tecnología de reputación web, un componente clave de la infraestructura Trend Micro Smart Protection Network, que lleva funcionando desde hace casi dos años a través de una de las bases de datos de reputación de dominios más grande del mundo. La tecnología previene tanto a usuarios como a aplicaciones de acceder a páginas web infiltradas o maliciosas mientras estén conectados o no a la red corporativa.



La amenaza de fuga de datos empresariales

DeviceLock, y SecurStar han sacado al mercado una solución de seguridad de punto final integrada, gestionada centralmente que hace frente al reto de frenar el traspaso no autorizado de datos de los ordenadores de la empresa a dispositivos de memoria extraíbles no encriptados y a otros dispositivos, como USB, tarjetas de memoria flash y CD/DVD. El software de control de acceso a dispositivos/puertos DeviceLock 6.4.1, aporta la capacidad de permitir o negar el traspaso de datos en función de si los datos están encriptados de forma segura con el programa DriveCrypt Plus Pack Enterprise (DCPPE) 2.3.11 de SecurStar. Cuando DeviceLock y DriveCrypt estén instalados en el mismo ordenador de punto final, todo la encriptación de datos, así como las funciones de administración de contraseñas y claves centralizada, las realiza DriveCrypt, mientras que la característica 'Crypto Intelligence' de DeviceLock comprueba la encriptación de los datos que se traspasan a dispositivos de almacenamiento y activa las políticas de control de acceso que correspondan. Por ejemplo, algunos empleados de sus grupos pueden estar autorizados para escribir y leer datos de tabletas flash USB únicamente si se han encriptado con DriveCrypt. Otros usuarios pueden estar autorizados solo a leer de dispositivos de almacenamiento extraíbles pero no a escribir en ellos, aunque exista encriptación. Con este enfoque centrado en los datos, las organizaciones pueden tener la tranquilidad de que la información corporativa contenida en dispositivos extraíbles o dispositivos de memoria está protegida por un encriptación que evita el acceso no autorizado a los datos en el caso de que se perdiera o robara un dispositivo con información.

Trayectoria híbrida en la adopción de Cloud Computing



El número de empresas que planean la integración y prueba de Cloud ha aumentado enormemente, según un estudio reciente encargado por Avanade, proveedor de servicios de tecnología de negocios. Los encuestados que afirman que están empezando a adoptar el Cloud Computing aumentaron más del 320 por ciento desde enero de 2009. Y, a pesar de la coyuntura económica, las empresas también están aumentando sus inversiones en la adopción de nuevas tecnologías (40 por ciento a nivel mundial). Este estudio, realizado por Kelton Research, recoge que las empresas que indican que no tienen planes de adoptar el Cloud Computing se han reducido del 54 por ciento al 37 por ciento. Más del 70 por ciento de las empresas del mundo señalan que la economía o bien ha ayudado (13 por ciento) o no ha tenido efecto (58 por ciento) en los esfuerzos para implementar el Cloud Computing. Más de la mitad de los encuestados están recurriendo a una mezcla de sistemas de TI internos (locales) y basados en Cloud. Hay una tendencia clara a usar estos despliegues híbridos de sistemas basados en Cloud a medida que las empresas se encuentran más cómodas con las nuevas tecnologías.

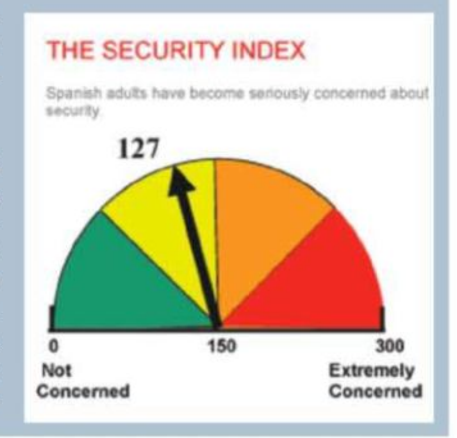
Aunque la seguridad sigue siendo la principal preocupación para las empresas que están considerando el Cloud, el 40 por ciento de las empresas mundiales que utilizan el Cloud Computing informan que otro problema principal es la alta curva de aprendizaje del personal de TI. Y más del 35 por ciento tienen la experiencia de un corte de servicio en la empresa proveedora del servicio.

Los españoles desconfían de la capacidad de las Administraciones Públicas para salvaguardar datos personales

Unisys ha hecho pública la quinta oleada de su Índice de Seguridad en lo que a la percepción de seguridad de los consumidores se refiere, y que muestra unos de los datos más optimistas desde la primera oleada, realizada por la compañía en agosto de 2007. De hecho, el 66% de los españoles muestra poca o ninguna preocupación sobre la seguridad personal de aquí a seis meses vista. Según los datos del Índice, que se realizó en España a 1.006 personas de más de 18 años durante el pasado mes de septiembre, la mayor preocupación concreta de los españoles es el fraude con tarjetas de crédito y los riesgos de una epidemia masiva.

Sobre una cifra máxima de preocupación de 300, los españoles muestran una inquietud global de 127 frente al 151 de la última oleada llevada a cabo en marzo de 2009. Por áreas, la seguridad financiera (que incluye el hecho de que otras personas obtengan y utilicen las tarjetas de crédito propias o las capacidad de asumir las obligaciones financiera), con un índice de 148; y la seguridad nacional (que incluye no sólo seguridad en España sino la posibilidad de que nos afecte una epidemia masiva), con un 145, representan las mayores preocupaciones. Por el contrario, la seguridad en Internet, con un índice de 86, no supone mayor preocupación en nuestro país.

En general, sólo una persona de cada diez está preocupada con su seguridad personal, lo que no representa ningún cambio desde la primera oleada. Además el 76% de los españoles se muestran preocupados o muy inquietos con el uso que hacen los bancos de los datos privados de sus clientes mientras que el 69% de los españoles desconfía de la utilización de la información personal que realizan las Administraciones Públicas. Tan sólo el 9% confía plenamente, por lo que tanto el Gobierno como los bancos deberían trabajar en mejorar la percepción de los ciudadanos hacia este tipo de instituciones.



BitDefender Antivirus 2010 obtiene la certificación Advanced+

BitDefender recibe el máximo galardón otorgado por AV-Comparatives a su solución de seguridad BitDefender Antivirus 2010 por su alto nivel de detección y bajo índice de falsos positivos. El análisis, realizado el pasado mes de agosto de 2009 entre 16 soluciones antivirus, se llevó a cabo introduciendo una serie de muestras, tanto limpias como maliciosas, para ser evaluadas por las soluciones de seguridad mediante su configuración por defecto, en primera instancia, para luego repetir dicha acción con su configuración más avanzada. Para clasificar los resultados obtenidos, AV-Comparatives utilizó un sistema de puntuación basado en 4 niveles, de menor a mayor eficacia: Tested, Standard, Advanced y Advanced+.

Datos confidenciales en ordenadores portátiles sin seguridad lógica

El 48% de las empresas reconoce que no dispone de ningún tipo de mecanismo para detectar y evitar fraudes corporativos tales como la competencia desleal, la fuga de información, el espionaje industrial, la segregación de funciones, etc. Así lo determina un estudio realizado por Grupo Paradell, Detectives Privados y Consultoría de Riesgos, basado en la información obtenida de entre 800 empresas a nivel nacional.

A pesar de la falta de prevención de fraudes por parte de las corporaciones, casi el 80% de los gerentes encuestados cree que la mejor estrategia para prevenirlos es a través de la función compliance (auditorías internas integrales en riesgos operacionales) y más del 90% de los mismos estarían dispuestos a aplicar fuertes medidas disciplinarias. De hecho, el 77% de organizaciones encuestadas reconoce que maneja datos confidenciales en equipos portátiles sin ningún tipo de seguridad lógica y desconoce las consecuencias que acarrearía que esta información llegara a terceras personas y el uso que se podría hacer de ella.

Un 30% de los fraudes que se cometen en las empresas españolas está relacionado con la fuga de datos confidenciales. La fuga de información de carácter confidencial es la tipología de fraude corporativo que más ha aumentado en España, hasta un 60% respecto al año pasado (datos extraídos del Informe Fraude elaborado por Grupo Paradell, basado en las aproximadamente 4.000 investigaciones anuales que realiza la firma a nivel nacional).

Máxima seguridad de sus datos a gobiernos y empresas



Kingston Digital ha alcanzado un acuerdo con SPYRUS, compañía de desarrollo y fabricación de hardware encriptado, autenticación y productos de seguridad para contenidos digitales. Según los términos de este acuerdo, Kingston Digital incorporará la tecnología de seguridad patentada por SPYRUS en sus dispositivos USB Flash Kingston DataTraveler con el objetivo de ofrecer a instituciones gubernamentales y empresas de todo el mundo nuevos niveles de seguridad y encriptación.



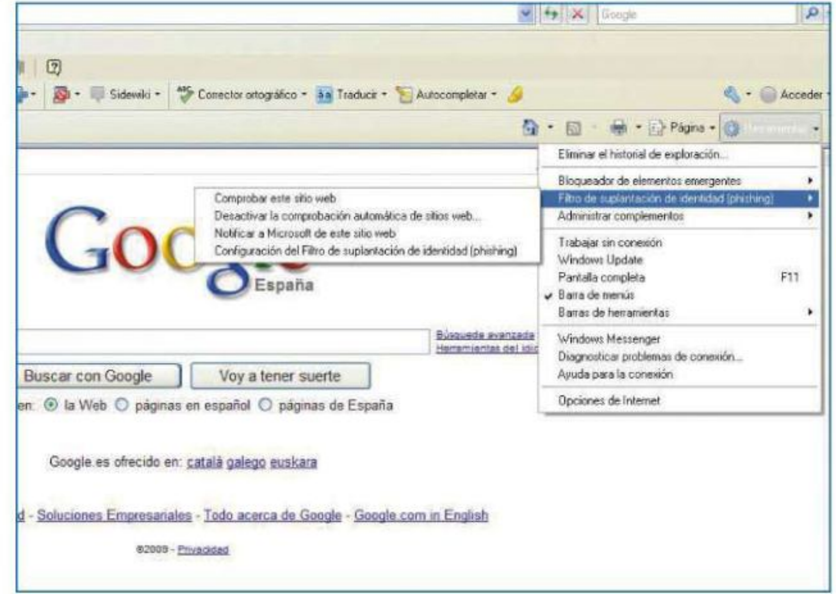
Ladrones de identidad

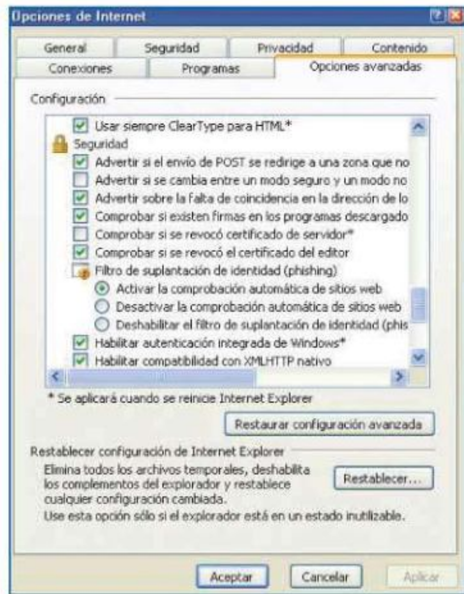
Tras el término de phishing se esconde un tipo de ingeniería social cuyo propósito es adquirir información confidencial de los usuarios de manera fraudulenta. Repasamos las distintas manifestaciones que esta estafa puede llegar a adoptar.

PandaLabs en su último informe trimestral (julio-septiembre de 2009) ha constatado una actuación récord de los hackers a la hora de crear nuevas amenazas. La compañía, en concreto, habla de cinco millones de amenazas en tan sólo tres meses. En este contexto, se recoge un aumento del número de troyanos (en un 71%) seguido del adware (13%) y el software espía (9%). Precisamente, las tendencias que PandaLabs ha analizado y estudiado han corroborado un crecimiento destacado de la propagación de software malicioso a través de las ya populares redes sociales (Twitter o Facebook, entre otras), correos basura y técnicas de posicionamiento de páginas web a través de las cuales el internauta llega a sitios falsos.

Con estos números puestos sobre la mesa, no es de extrañar que los usuarios estén ya habituados a las distintas formas que los códigos malintencionados pueden adoptar. Uno de éstos es el phishing, relacionado con una clase de delito cibernético (y técnica de ingeniería social) vinculada a las estafas, y más en concreto, a aquéllas relacionadas con los fraudes que se producen en Internet. La práctica más conocida y, quizá, más extendida del phishing tiene a la banca como protagonista, aunque como veremos en el siguiente artículo existen otras manifestaciones. A pesar de que en la actualidad las noticias relacionadas con este delito suelen ser bastante habituales, tenemos que tener en cuenta que las primeras informaciones relacionadas con el phishing datan del año 1.996. Desde entonces, los ataques se han venido sucediendo de manera casi indiscriminada con el único propósito de causar importantes pérdidas económicas a las potenciales víctimas. Especialmente revelador es un estudio llevado a cabo por la empresa japonesa Trend Micro y en el que han participado 1.000 usuarios mayores de 18 años y con un teléfono inteligente en su poder: se ha revelado que éstos no parecen estar







Aquí, en ambos casos, mostramos cómo protegerse.

demasiado preocupados ante la posibilidad de sufrir un ataque de phishing, y que sólo un 23% emplea software de seguridad ya integrado en sus teléfonos. El informe también se hace eco de que el 80% de los usuarios sabe en qué consiste y un 20% de los mismos dice haberse encontrado con algún fraude de phishing. De igual forma, conviene tener en cuenta el siguiente dato aportado por la APWG (Anti-Phishing Working Group): el número de páginas web afectadas por este delito en junio de 2009 se elevó a 49.084, el número más alto desde abril de 2007 cuando se registraron 55.643 sitios.

¿Por qué la denominación de phishing? Los orígenes de la palabra están ligados al término inglés "fishing". Con él, se alude al intento de los estafadores (también conocidos como phisher) para que los internautas piquen finalmente el anzuelo. En este caso, una persona con identidad falsa despliega un conjunto de técnicas que le llevan a hacerse pasar por una institución, entidad o empresa a priori de confianza.

Con esta suplantación, el objetivo no es otro que obtener una serie de datos de carácter personal del usuario con el que se pone en contacto (siempre mediante la fórmula del engaño): este es el caso del número de la tarjeta de crédito o la cuenta bancaria, la contraseña que le permite tener acceso a su correo electrónico personal, etcétera. Cuando el estafador tiene ya está información en su mano, el siguiente paso es hacer un uso fraudulento de ella para ganar la máxima cantidad de dinero posible.

Métodos más empleados

El funcionamiento del phishing se basa principalmente en el envío de mensajes

>>> TEN EN CUENTA QUE...

1. **Los métodos que utilizan las personas que practican phishing suelen llevarse a cabo a través de solicitudes con un carácter urgente y alarmista que invitan a una rápida respuesta.**
2. **El correo web es la herramienta más utilizada en estos casos y los sitios a los que redirigen al internauta dan la sensación de ser legales. Conviene ser ante todo ser precavido y extremar las medidas de seguridad oportunas.**
3. **Los correos fraudulentos suelen tener características comunes como detalles en los pies de página y en el encabezado. Son correos que, de igual forma, no están personalizados.**
4. **Las entidades bancarias nunca solicitan a través del correo electrónico las claves a sus clientes. Tampoco lo hacen vía telefónica.**
5. **No se debe hacer clic en los enlaces que se incluyen en los mensajes de los e-mail. Es preferible que nosotros mismos tecleemos la dirección de la página a visitar, sobre todo en los casos en los que vamos a introducir información confidencial.**
6. **En el caso de tener alguna duda o pregunta, lo más aconsejable es que nos dirijamos personalmente a la entidad que aparentemente nos ha enviado el mensaje.**

>>> ¡OJO AL CANDADO!

En el caso de que no sea posible fiarse de una página web por su barra de direcciones, incluso en el supuesto de que está incorpore la imagen corporativa del sitio que dice ser, uno se plantea lo siguiente: ¿Cómo puedo saber que el portal que estoy visitando es seguro al cien por cien? La clave está en el empleo de los sistemas de cifrado que transmiten la información personal. En el caso de Internet Explorer esto se comprueba a través del icono de color amarillo que se encuentra en la barra de estado y que adopta la forma de un candado. Si hacemos doble clic sobre éste el nombre que tendría que aparecer tras el campo "Enviado a" debería coincidir con el del sitio en el que nos encontramos. Algunos navegadores sitúan este candado en la barra de navegación superior.

falsos a través del correo electrónico que, a simple vista, parecen provenir de páginas web de confianza y fácilmente reconocibles. El ejemplo más típico y representativo es el banco o la caja de ahorros donde tenemos depositado nuestro dinero. Los phisher, en este caso, se las ingenian para hacer creer al uinternauta que, efectivamente, su banco se está dirigiendo a ellos y que deben cumplimentar una serie de datos y requisitos a través de una página de Internet que a primera vista da la sensación de resultar legal.

Así, una de las técnicas más empleadas, y a las que suelen recurrir, consiste en incluir en este tipo de correos un enlace o link que, en lugar de redireccionar a la página legítima, redirige a otra que resulta que es un timo. ¿El resultado? La víctima introduce los datos que se la solicitan (el número de su cuenta personal, por ejemplo) y los estafadores se hacen con ellos sin que ésta se percate de que la están robando su identidad. Los enlaces a los que esta víctima es enviada suelen contener direcciones URL que están mal escritas, y algunas contienen el carácter de la letra @.

También es habitual que el cuerpo de texto de estos correos tengan faltas ortográficas o frase inconexas o carentes de concordancia. Existen estafadores que, de igual forma, utilizan comandos en javascript, un tipo de lenguaje que puede alterar la barra de direcciones del navegador web cuando nos adentramos en Internet.

Prácticas

Tal y como hemos señalado, la imagen más típica que se tiene del phishing está relacionada con aquélla en la que el usuario recibe un mensaje de su entidad bancaria solicitándole sus claves de acceso personal vía web. Uno de los motivos más alegados de esta petición hace referencia al hecho de que la entidad en cuestión está procediendo a diversos cambios en sus sistemas informáticos que "exigen" al cliente la introducción de información privada como passswords y códigos PIN, entre otros. Ante una situación de este tipo, es importante tener en cuenta que los bancos bajo ninguna circunstancia actúan ni actuarán de esta manera (ni siquiera vía telefónica) con sus clientes. Nunca les



>>> LA IMPORTANCIA DE LA CERTIFICACIÓN SSL

Del inglés Secure Sockets Layer, protocolo de capa de conexión segura, la certificación SSL es una norma que emplea la criptografía para proporcionar una comunicación segura a través de Internet. SSL tiene la capacidad de proteger los datos que se transfieren vía http a través del cifrado que las páginas de Internet emplean. La estructura de esta certificación se asienta en dos claves.

Una que es pública y que sirve para cifrar la información y otra de carácter privado. A este respecto, son muchos los portales (este es el caso de los bancos como Ibercaja o Caja Madrid) que para garantizar la plena seguridad de sus clientes utilizan este sistema de autenticación.

Se reconoce fácilmente porque en la barra de direcciones donde aparece la URL en vez de mostrarse la expresión "http" el internauta va a encontrarse con esta otra: "https". En nuestro país, la empresa VeriSign es un destacado proveedor de servios SSL.



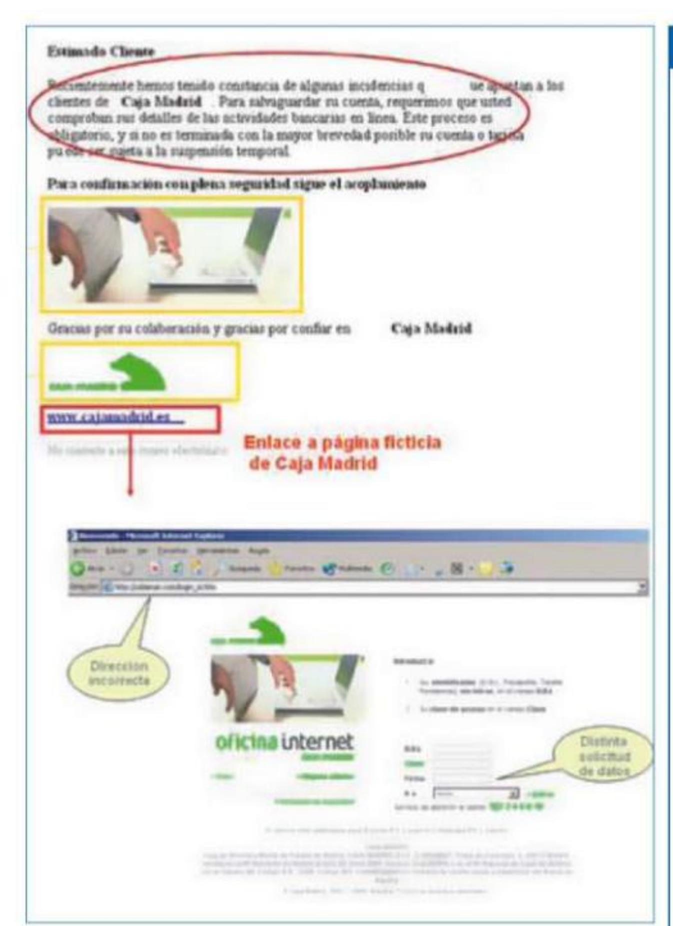
>>> CÓMO PROTEGERSE

En el mercado, es posible encontrar diversos programas informáticos que están preparados para identificar el phising. Asimismo, algunos de ellos pueden integrarse como una barra de herramientas dentro del propio navegador web que el ordenador tiene instalado y que revela el dominio real de la página que se está visitando. En este sentido, por ejemplo, Microsoft Internet Explorer 7 ya introdujo el llamado filtro de suplantación de identidad para ayudar al internauta a identificar los sitios que se dedican a suplantar la identidad de las organizaciones. Dando un paso más, la versión de Internet 8 perfeccionó esta característica introduciendo un filtro de pantalla inteligente. Se llama SmartScreen y sirve para protegerse de la instalación de aquellos códigos maliciosos y programas malintencionados que ponen en peligro la privacidad e identidad de los usuarios y sus datos más valiosos. Si este filtro está activado y se intenta acceder a una página web que no es completamente segura se muestra una ventana emergente informando de este hecho. Lo mismo sucede cuando intentamos instalarnos herramientas y aplicaciones potencialmente no seguras. Ahora bien, ¿qué queremos complementar la seguridad de nuestro navegador? Es posible adquirir programas gratis como CyberDefenderFREE, disponible en el siguiente enlace: http://cyberdefender.com/early_spy_feature.html. También puedes probar el software Phisguard (www.downloadsoftware4free.com/publisher/phishguard-corporation).

van a pedir cambios en sus claves a través de los procedimientos descritos.

Más allá del uso del correo electrónico, este tipo de fraude ha comenzado a adoptar otras formas y actuaciones. Una de éstas tiene que ver con el teléfono y el empleo de la VoIP (llamadas telefónicas más económicas a través de Internet). En este caso, las posibles víctimas suelen encontrarse en su contestador con una voz que les informa que deben llamar al número que a continuación se les comunica porque su banco ha congelado su cuenta personal.

Otra táctica consiste en el envío de correos electrónicos en el que, supuestamente, es la propia entidad la que solicita a sus clientes que llamen a un número en concreto: un mensaje grabado y con un contenido completamente falso le requerirá el mayor número de datos privados posibles. A este listado hay que sumar también el intento de estafas a través de mensajes de texto corto y llamadas telefónicas en las que el emisor suplanta a entidades como, por ejemplo, la Agencia Tributaria de España (AEAT). Precisamente, la compañía Trend Micro detectó hace unos meses el envío masivo de correos electrónicos procedente en teoría

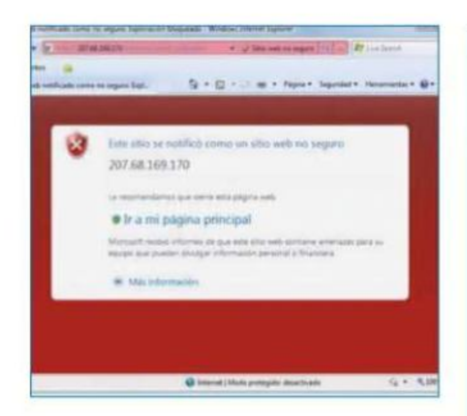


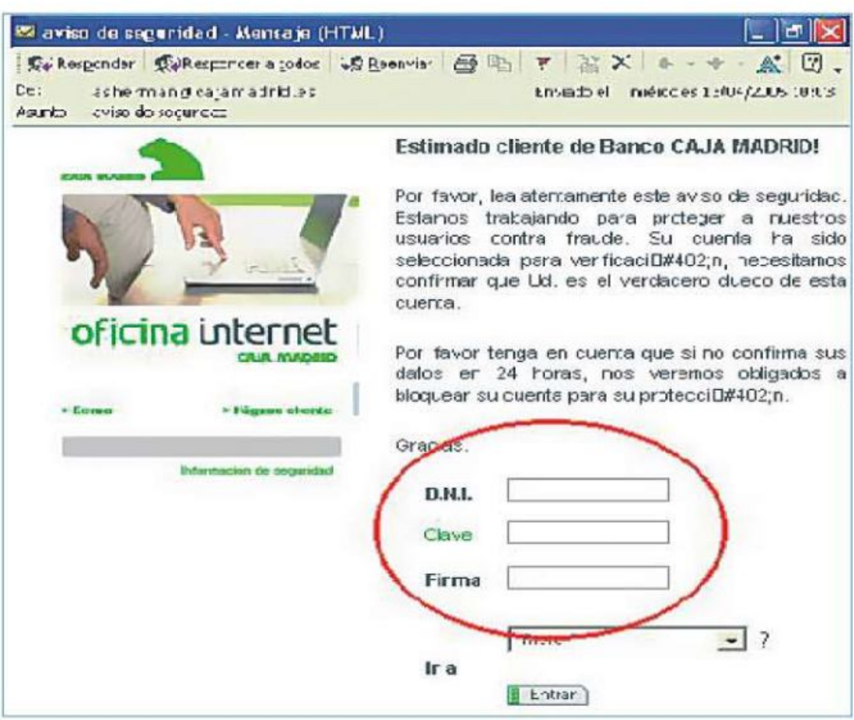
Ejemplo de mail fraudulento

>>> LA ACTUALIZACIÓN DE LOS TROYANOS

Panda Security en su Boletín Pandalabs "Datos bancarios al descubierto" ha ratificado que una de las preocupaciones mayores de los internautas en Internet tiene que ver con el robo de la información confidencial, sobre todo cuando se trata de datos bancarios. A este respecto, los troyanos bancarios son una de las clases de malware o software malintencionado más peligroso porque están pensados para robar este tipo de datos. De entre los troyanos más peligrosos que la firma recoge nosotros hemos destacado los siguientes:

- **Banbra.FTI: Se manifiesta en el ordenador haciéndose pasar por una imagen que reproduce un recibo bancario y consigue ejecutarse en un segundo plano en el ordenador del usuario. Con esta técnica, se consigue que la atención del usuario se desvíe hacia la imagen que aparece en la pantalla. Para conseguir los datos bancarios, este troyano habilita la opción que permite guardar las contraseñas que han sido introducidas en el navegador de Internet Explorer. Esto permite, con posterioridad, acceder al directorio en el que quedan guardadas las contraseñas, sustrayendo aquellas vinculadas a entidades bancarias.**
- **Banker.LAX: Para reforzar la seguridad y garantizar la tranquilidad de sus clientes los bancos han desarrollado tarjetas de coordenadas, las cuales tienen un conjunto de unas 60 claves aproximadamente. Tienen la ventaja, además, de que aún en el caso de que el ciberdelincuente obtenga la clave de acceso le será imposible realizar ningún movimiento en la cuenta de su víctima porque, en este caso, se le pedirá además una segunda claves seleccionada de manera aleatoria de esta tarjeta de coordenadas. El problema se plantea en el instante en que se diseña un troyano tipo Banker.LAX (cuenta con un listado de direcciones web de los bancos que monitoriza) al solicitar todas las claves de esta tarjeta. En este caso, cuando el usuario accede a la página que coincide con la de la lista del ciberdelicuente es redirigido a una página que imita a la que es la original.**





de la AEAT con el asunto "Reembolso de Impuestos". En el contenido de este mensaje se comunicaba a los destinatarios que su declaración de impuestos había sido elegida para una devolución de 186,80 euros y que para solicitar este reembolso era necesario rellenar un formulario. Y en lo que respecta a la VoIP, los estafadores han desarrollado programas capaces de crear centralistas con fines también engañosos y fraudulentos.

El phishing desde otra perspectiva

Poco a poco este tipo de estafas han ido derivando a otras variantes cuanto no menos peligrosas. Este es el caso de las ofertas falsas de vehículos. Responden al concepto de phishing car y básicamente consisten en captar a personas que quieren comprar un automóvil a cambio de un precio bajo. El resultado es que la venta nunca llega a realizarse y que la persona que efectúa el pago como señal (entre un 30% y un 40% aproximadamente) al final se queda sin su dinero y sin el automóvil en el que estaba interesado.

>>> EL TRABAJO DE LOS FABRICANTES DE ANTIVIRUS

Los principales fabricantes de programas antivirus como Symantec, Panda Security, G-Data o McAffe, entre otros, cuando lanzan sus productos ya incorporan funciones de seguridad que permiten que los usuarios refuercen el blindaje de sus equipos y eviten ataques como el phishing. En el caso de McAfee, la firma norteamericana ha desarrollado un complemento de carácter gratuito para navegadores web que propone asesoramiento sobre diferentes aspectos vinculados a la seguridad de las páginas que se visitan antes de hacer clic en ellas. Se trata de SiteAdvisor, es gratuito y muy fácil de utilizar ya que emplea un conjunto de pequeños iconos de clasificación de los sitios que el internauta visita en base a estas valoraciones y recomendaciones: riesgo bajo o inexistente, riesgo leve, riesgo grave y desconocido, sitio todavía no clasificado que exige prudencia. El análisis de cada una de las páginas se basa en el trabajo que McAfee lleva a cabo a lo largo de todos los días, entrando en los portales y probándolos para detectar la posible presencia de cualquier amenaza, y entre las que el phishing se encuentra. www.siteadvisor.com/howitworks/index.html

En este tipo de timos el cebo son coches lujosos que se venden a precios muy atractivos y tentadores. Hay estafadores que, a este respecto, recurren a páginas web falsas (otros anuncios de segundamano) con nombres de empresas que se dedican a este negocio y con portales muy similares a los de verdad.

Es habitual que quienes practican el phishing car vendan los automóviles fuera del país por lo que no existe la opción de verlos personalmente. También es común que los pagos se efectúen a través de organizaciones de envio de dinero fuera del propio país.

Otra de las técnicas empleadas es el pharming y se refiere a la manipulación de las direcciones DNS (Domain Name System, sistema de nombre de domino) de los ordenadores que derivan el tráfico web de un sitio a otro falso para intentar obtener claves de acceso. Existen troyanos y gusanos que llevan a cabo este tipo de actuaciones. Finalmente, también hay que tener en cuenta los premios de lotería falsa que se notifican a través del correo electrónico y las páginas web también falsas de recargas que suelen localizarse en algunos anuncios de los enlaces patrocinadores de los buscadores de Internet.


[* 06.05 *]Reembolso de Impuestos - Mensaje (HTML)

Archivo Edición Ver Insertar Formato Herramientas Acciones ?

Responder | Responder a todos | Reenviar

Mensaje reenviado el 01/09/2009 16:02.

De: Agencia Tributaria [impuestos@aeat.es]
Para: undisclosed-recipients:
CC:
Asunto: [* 06.05 *]Reembolso de Impuestos

Agencia Tributaria — GOBIERNO DE ESPAÑA

Notificación de Impuestos

Después de los cálculos del último informe anual de su actividad fiscal hemos Determinado que usted es elegible para Recibir un reembolso de impuestos de 186.80 euros.

Por favor, envíe la solicitud de reembolso de impuestos y nos permiten 3 días para procesarla.

Para acceder al formulario para su reembolso de impuestos, haga clic aquí

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación de los registros inválidos o aplicándose después del plazo.

Documento de Referencia: (92054568).

Ejemplo fraude

Víctimas que se convierten en estafadores sin saberlo

Además de enriquecerse con el dinero de sus víctimas, los estafadores recurren también a la práctica del phishing para blanquear dinero. A esto se le conoce como scam o phising laboral y hace referencia a la captación de personas en las que empresas ficticias les ofrecen la posibilidad de trabajar desde casa con el aliciente de cobrar cuantías económicas muy jugosas (para ponerse en contacto con sus víctimas, los estafadores además de recurrir a mensajes de correo que resultan ilusorios suelen adentrarse en foros, salas de chat, anuncios de páginas web de trabajo, etcétera). Pero lo que estas víctimas desconocen es que detrás de toda esta infraestructura se esconde una red que, precisamente, les van a utilizar para blanquear dinero procedente de estafas bancarias (se convierten, por lo tanto, en partícipes de un delito).

Para captar la atención de las personas, estas organizaciones recurren a llamadas muy tentadoras del tipo: ¿Desea trabajar desde su casa cómodamente?, ¿Quiere obtener dinero de una forma rápida?, ¿Está en paro y desea trabajar? Para que la oferta de trabajo sea más creíble se envía un contrato (siempre falso) en el que hay cumplimentar una serie de campos de carácter obligatorio.

"Ellos ya hablan Inglés. Y usted... ¿cuándo?"



"Fue muy sencillo desde el principio. En menos de un año, he aprendido a hablar y a escribir en inglés."

Hanny



"Yo es que tenía la fama de que nunca iba a hablar inglés. ¡Y este Método me está funcionando!"

Manel



"...Incluso hablo por teléfono en inglés. Este Curso ha sido definitivo para mi trabajo".

Olivia

"¡A las pruebas me remito. Con mi Método, El Inglés con Mil Palabras usted aprenderá inglés, se lo garantizo!"

Profesor Maurer

Y ahora CCC te financia tus estudios hasta en 2 años y sin intereses.

CCC 70 AÑOS Formando profesionales

www.cursosccc.com

902 20 21 22

"El Inglés con Mil Palabras"
www.miraloquedicenlosalumnos.com

OTROS CURSOS CCC

IDIOMAS
- Curso de Chino Mandarin con la Profesora Yang Yun
- Francés

ACCESO A ESO Y UNIVERSIDAD
- Graduado ESO, Preparación al Título Oficial
- Acceso a la Universidad para Mayores de 25 años
- Acceso a Ciclos Formativos de Grado Superior y Grado Medio

PROFESIONES SANITARIAS
- Auxiliar de Enfermería FP
- Tco. Superior en Educación Infantil FP
- Auxiliar de Jardín de infancia
- Tco. en Farmacia y Parafarmacia FP
- Técnico en Atención Sociosanitaria FP
- Auxiliar de Geriatría
- Técnico Superior en Dietética y Nutrición FP

PROFESIONES TÉCNICAS
- Técnico en Frío y Climatización FP
- Técnico Instalador de Equipos de Energía solar
- Técnico en Construcción de Obras
- Instalador Electricista FP
- Mecánica del Automóvil FP

BELLEZA Y MODA
- Peluquería FP
- Esteticista Profesional FP

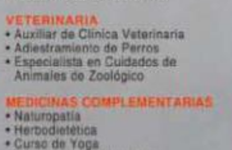
EMPRESA E INFORMÁTICA
- Microsoft Office Formación Personalizada
- Tco. Superior en Administración de Sistemas Informáticos FP
- Webmaster
- Administración de Empresas
- Técnico Superior en Gestión Comercial y Marketing FP
- Técnico Superior en Secretariado FP
- Auxiliar Administrativo FP

ARTES Y DECORACIÓN
- Fotografía Digital
- Decoración
- Monitor/a de Manualidades

VETERINARIA
- Auxiliar de Clínica Veterinaria
- Adiestramiento de Perros
- Especialista en Cuidados de Animales de Zoológico

MEDICINAS COMPLEMENTARIAS
- Naturopatía
- Herbodietética
- Curso de Yoga
- Monitor/a de Relajación y Desarrollo Personal

OTROS CURSOS
- Guitarra
- Curso de Pilates
- Profesor de Educación Vial
- Técnico en Cocina y Gastronomía FP
- Máster en Protección Civil



FP Cursos que te preparan para presentarte al examen y obtener el título oficial FP

Deseo recibir información detallada del curso:

Nombre: .... Apellidos: ....

E-mail: ....

Teléfono: ..../.... Fecha nacimiento: ..../..../....

Domicilio: .... Nº: .... Piso: ....

Población: .... C.P.: .... Provincia: ....

DNI (opcional): .... País de nacimiento: ....

Para más información, envía este cupón a CCC: Apdo. 17222 - 28080 Madrid | 8N5

Te informamos que los datos que nos has suministrado pasarán a formar parte del fichero automatizado de Centro para la Cultura y el Conocimiento S.A. con dirección en C/ Orense 20-1º (28020) de Madrid , a donde te podrás dirigir para ejercitar en cualquier momento tus derechos de acceso, rectificación, cancelación u oposición al tratamiento de los mismos. A través del envío del presente formulario nos das tu consentimiento expreso para que tus datos sean tratados para hacerte llegar la información que nos has solicitado. Y también para que te podamos enviar o realizar comunicaciones comerciales por cualquiera de los medios que nos hayas facilitado de CCC, salvo que nos indiques lo contrario marcando esta casilla ☐ y de otras empresas relacionadas con los sectores de telecomunicaciones, financiero, ocio, formación, gran consumo, automoción, energía, agua, ONGs e instituciones y organizaciones públicas, salvo que nos indiques lo contrario marcando esta casilla ☐ (Ley orgánica 15/1999 de 13 diciembre de Protección de Datos).

















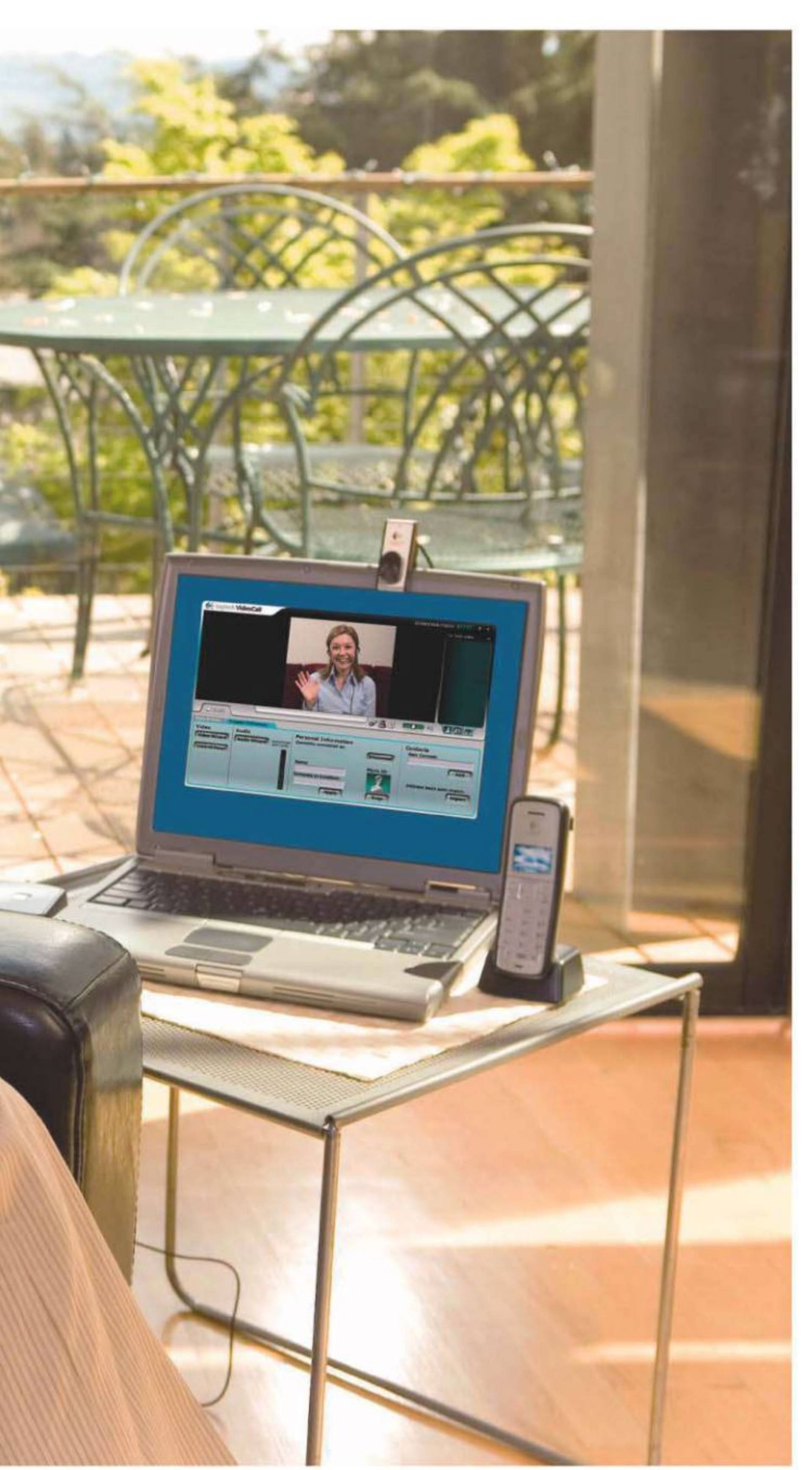








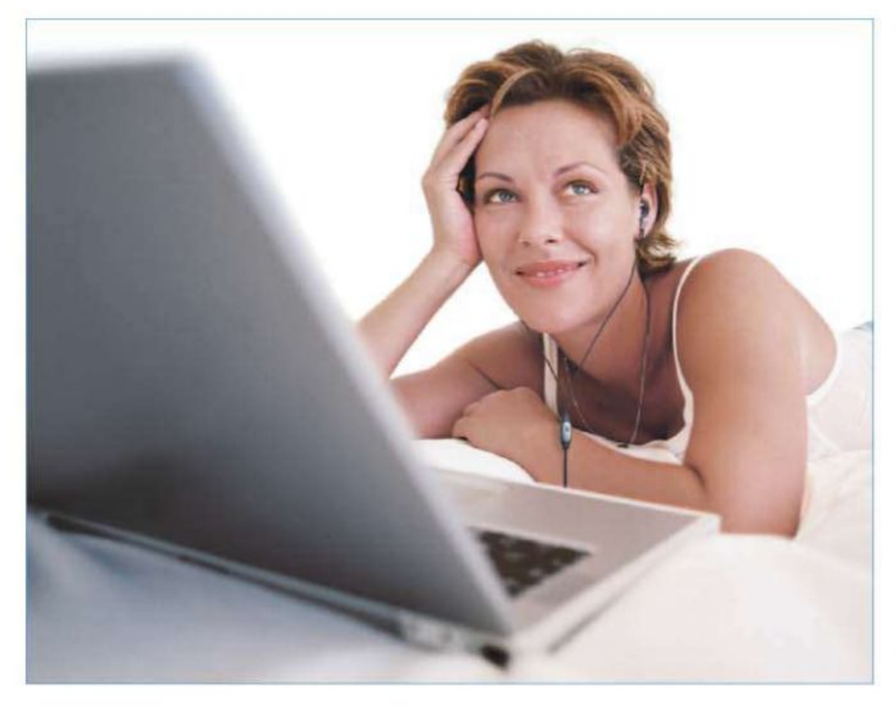
Riesgos en las comunicaciones sobre VoIP



Las redes VoIP han supuesto un gran avance en la tecnología de telecomunicaciones: su uso es cada vez más frecuente y las mejoras técnicas que experimenta son constantes. Las amenazas también son, por su parte, cada vez mayores. Denegación de servicio, fraude, suplantación de identidad, etcétera. ¿Existe alguna manera de protegerse de estos riesgos?

VoIP es el acrónimo de Voice over Internet Protocol, un término que hace referencia al envío de paquetes IP sobre redes de datos. De esta manera, logra la convergencia de dos mundos hasta hace poco separados: la transmisión de voz y el envío de datos. Su fin es la transmisión de voz previamente procesada y encapsulada en paquetes que pueden transportarse fácilmente a través de la Red. Su descubrimiento ha supuesto una gran cantidad de ventajas tanto para los particulares como para las empresas, siendo la principal el ahorro de costes que se deriva de la disminución de las infraestructuras necesarias y del mantenimiento de las mismas. Y es que, mientras que una centralita telefónica implica contar con un gran número de teléfonos conectados todos a través de un cableado o fibra óptica, una comunicación a través de IP tan sólo requiere comprimir la voz y enviarla en paquetes de datos a través de una línea que es capaz de soportar diferentes llamadas e incluso diferentes datos sin desaprovechar el ancho de banda.

Su estructura básica la conforman tres elementos principales: los terminales, que son los dispositivos que utilizarán los usuarios para comunicarse y que, aunque mejorados tanto en hardware como en software, realizan las mismas funciones de los teléfonos tradicionales; los gateways, que conectan las redes VoIP con las redes de telefonía tradiciones; y los gatekeepers, cuya labor es la de autentificar los usuarios, controlar la admisión, el ancho de banda, el encaminamiento, etcétera. Con esta sencilla estructura, el usuario es capaz de entablar una comu-





VOIP DECT 321 de Philips

nicación con cualquier punto del planeta pero también, como ahora pasaremos a explicar, se expone a varios riesgos.

Ataques contra la seguridad

A medida que el uso de la VoIP ha aumentado a gran velocidad, también lo han hecho las amenazas a las que se expone. Así pues esta tecnología es víctima de ataques que tendrán como objetivo no sólo el robo de información confidencial, sino también la degradación de calidad del servicio o la información y datos que se desprendan de la propia llamada, utilizando éstos de manera maliciosa con el fin de bombardear con spam, interceptar llamadas, reproducir conversaciones, etcétera.

El primer caso de ataque es el de los accesos desautorizados. Al incluir numerosos sistemas para el control de la llamada, administración o la facturación, los sistemas VoIP contienen gran cantidad de datos que pueden llevar a la existencia de fraudes. El acceso a información telefónica que incluya datos sobre la facturación, las cuentas o los registros pueden provocar, además, efectos devastadores para cualquier compañía. Y es que, una vez un hacker se ha adueñado de ellos, puede obtener acceso y realizar llamadas de larga distancia que supongan un elevado gasto. Asimismo, al apoyarse en unas redes potencialmente inseguras, como lo son de por sí las redes IP, gran cantidad de ataques hacia estas infraestructuras van a afectar irremediablemente a la telefonía. Uno de los mayores problemas que puede surgir es el eavesdropping, un término que se traduce como escuchar secretamente. Tal y como su nombre indica, consiste en interceptar las conversaciones VoIP por parte de terceros individuos desautorizados.

Una segunda posibilidad son los ataques de denegación de servicio que consisten en intentos de disminuir el rendimiento de la red e incluso impedir la utilización de la misma. Estos, que tienen una gran relevancia en cualquier intercambio normal de datos, repercuten mucho en las comunicaciones VoIP ya que al ejecutarse en tiempo real, la pérdida ocasional de paquetes consecuencia de la congestión hace inviable una conversación telefónica para la que siempre será necesaria la existencia de garantías en la calidad de servicio. Los ataques de este tipo se centran, principalmente, sobre las empresas. Algunas técnicas que emplean los piratas informáticos se basan en el envío de paquetes especialmente construidos para explotar alguna vulnerabilidad en el software o en el hardware

>>> LOS PASOS DEL HACKER

Cuando el pirata informático selecciona una red como objetivo, llevará a cabo una serie de pasos encaminados a recopilar toda la información posible sobre su víctima. Una vez hecho, tratará de averiguar cuáles son sus principales debilidades para aprovecharse de ellas. Para la primera etapa, se suele realizar un footprinting, que implica la obtención de toda la información pública posible del objetivo escogido. En caso de tratarse de una empresa o un profesional particular, utilizará Google donde podrá encontrar posiblemente los perfiles, direcciones de correo, contactos y teléfono. Estos datos ofrecerán información al hacker para poder realizar ataques de suplantación de identidad y/o ingeniería social. Más adelante una de las acciones más comunes es obtener la mayor cantidad de datos posibles de las máquinas y servicios conectados en la red atacada. Después de tener un listado de servicios y direcciones IP consistente, el hacker tratará de buscar agujeros de seguridad, vulnerabilidades y obtener la mayor información sensible de esos servicios para poder explotarlos y conseguir una vía de entrada.

del sistema, saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos. En este sentido, los más dañinos son los llamados DDoS o ataques de denegación distribuidos. Se trata de ataques DoS simples pero realizados desde múltiples computadores de forma coordinada y que, puesto que en una red VoIP existen multitud de dispositivos con funciones muy específicas, un ataque contra casi cualquier dispositivo de la red pueden afectar seriamente a todo el funcionamiento.

Asegurar la red

Para paliar los riesgos, nada mejor que tomar las medidas de seguridad adecuadas para, por lo menos, no facilitar la tarea a los hackers. En este sentido, existen una serie de consejos encaminados a asegurar una red VoIP. La primera de ellas consiste en mantener siempre actualizados los sistemas. Es imprescindible que el administrador esté al corriente de los nuevos parches que existen en el mercado y se encargue de aplicarlos sobre su sistema. De este modo, es imprescindible que se encuentre protegido por un cortafuegos así como por un completo sistema antivirus actualizado que prevenga de gusanos y troyanos. Estas herramientas detectan correctamente aquellos ataques contra el servicio y, en algunos casos, pueden servir incluso para prevenirse de amenazas DoS.

Además, es recomendable modificar los protocolos y configurar los dispositivos para que realicen una autenticación de todos aquellos mensajes que se intercambian. En las redes IP cobran una especial importancia la autorización: los





EasyCall de Logitec



Plantronics Savi Go




VIOP de Sennheiser



SkyPhone de NGS



VOIP DECT 433 de Philips

>>> PROTOCOLOS DE VOIP

Las redes VoIP engloban una inmensa cantidad de protocolos ya que deben ofrecer los mismos servicios que la telefonía tradicional en lo que se refiere a estándares y servidores. Los más importantes, sin embargo, son dos:

- **H.323: se originó para el intercambio de audiovisual en las redes de área local. Con el tiempo evolucionó hasta convertirse en un estándar VoIP. Parte de los especialistas lo definen como un conjunto de protocolos que cubre las distintas vertientes de la comunicación como el direccionamiento, la señalización, la compresión, la transmisión de voz o el control de la transmisión.**

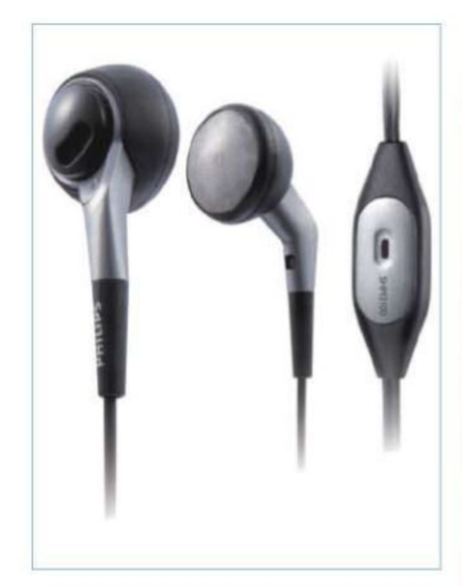
- **SIP: su simplicidad, escalabilidad y facilidad para integrarse con otros protocolos y aplicaciones lo han convertido en un estándar de la telefonía IP. Tan sólo maneja el establecimiento, control y terminación de las sesiones de comunicación. Normalmente una vez se ha establecido la llamada se produce el intercambio de paquetes RTP que transportan el contenido de la voz. Asimismo, encapsula también otros protocolos como SDP utilizado para la negociación de las capacidades de los participantes, tipo de codificación, etcétera. Su principal inconveniente es que es susceptible de ataques de secuestro de registro o de desconexión. Cabe destacar también entre sus desventajas que la sesión SIP llega a utilizar al menos tres puertos, de los cuales solo uno de ellos es estático, haciéndolo complicado de manejar desde el punto de vista de la seguridad ya que, por ejemplo, complica las políticas de cortafuegos.**

dispositivos deben tener limitados los grupos de elementos o direcciones IP de los que recibir tráfico web. Previniéndose ello, el usuario va a poder protegerse de manera muy eficiente contra los ataques de denegación de servicio. Asimismo, el cifrado es una medida necesaria que debe adoptar una infraestructura VoIP. El uso de TLS/SSL para establecer canales de comunicación seguros terminará con aquellos problemas que provengan del eavesdropping, manipulación y reproducción de los mensajes intercambiados. Además, los teléfonos VoIP pueden cifrar audio con el protocolo SRTP (Secure Real-time Transport Protocol), que ofrece confidencialidad, autenticación de mensajes y protección, haciendo frente a las amenazas de interceptación e inserción de audio.

Otra serie de precauciones que pueden tomarse son proteger y limitar el acceso a la red VoIP en la medida de lo posible, sobre todo desde el exterior. También limitar los volúmenes de datos y ráfagas



El VoIP Skype Calling Kit de IOGEAR



SHM3100 de Philips

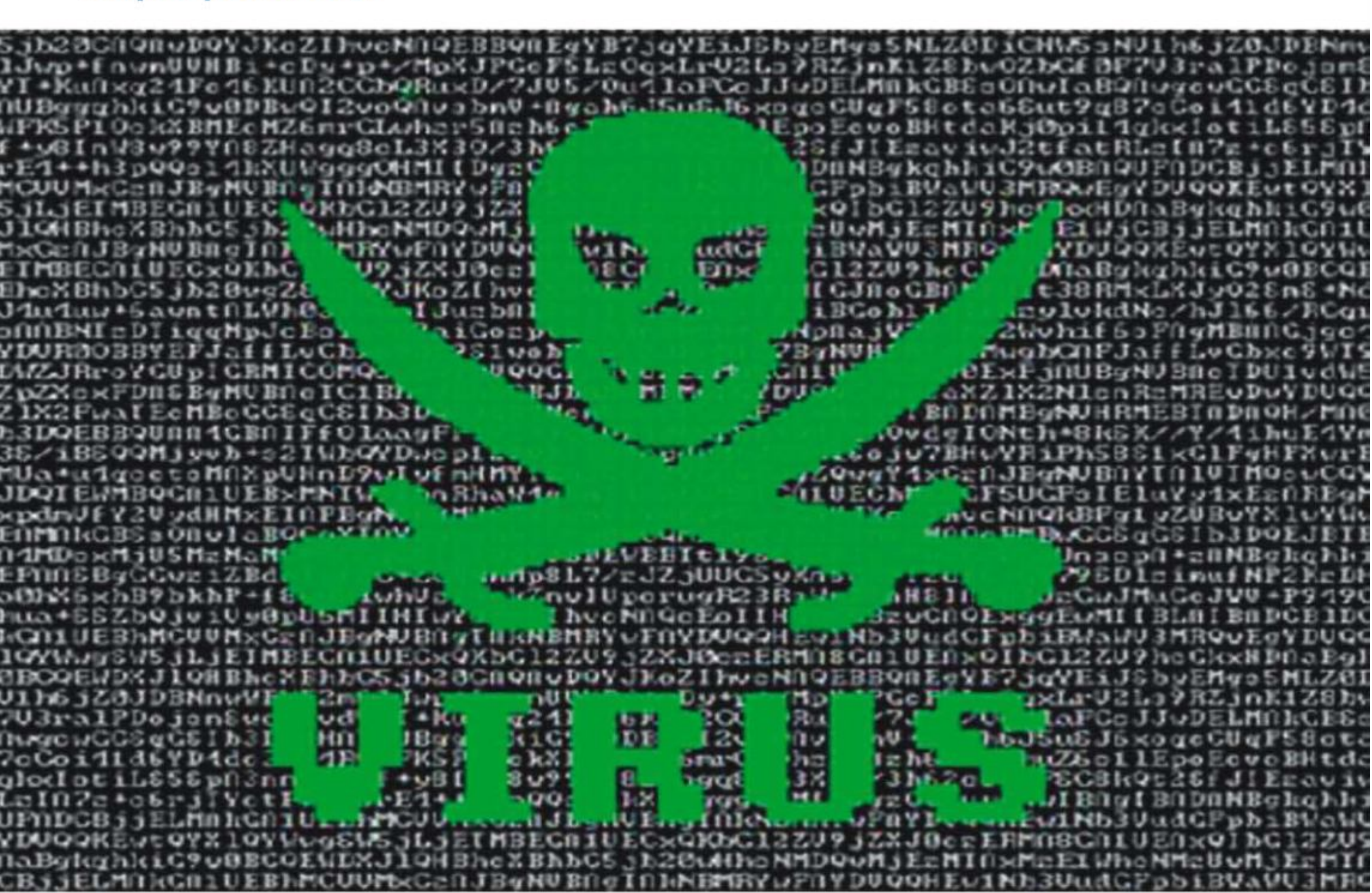


de paquetes en puntos estratégicos de la red para evitar gran cantidad de ataques DoS. Finalmente, otros consejos para protegerse de los ataques de enumeración pueden ser configurar correctamente los servicios para que no muestren más información de la necesaria, no usar nombres por defecto para archivos de configuración o cambiar la contraseña de todos los lugares.



Los “malos” llegan al móvil

El teléfono móvil se ha convertido en el objetivo prioritario de los ciberdelincuentes. No contentos con intentar el fraude y el ataque a través de las cuentas de correo electrónico, el envío de SMS infectados a los terminales es el nuevo objetivo de los ataques perniciosos.





Hasta hace poco, conseguir las contraseñas de correo electrónico de los usuarios o infectar el ordenador con algún virus maligno era la finalidad última de los ciberdelincuentes. Ahora son también los teléfonos móviles, los smartphones o teléfonos inteligentes el foco de tales agresiones. Con la proliferación en el mercado de dispositivos mejorados técnicamente, con mayores funcionalidades, más aplicaciones y enormes posibilidades de interactuar entre los usuarios se han convertido en un blanco fácil para este tipo de delincuentes. Principalmente, porque han evolucionado en pequeños ordenadores con los que se puede realizar un amplio número de acciones. De hecho, cuanto más "inteligente" y con más avances cuenta, el smartphone resulta más vulnerable y son mayores los riesgos de inseguridad que conlleva. Sobre todo, porque son muy pocos los usuarios que han dotado a su terminal de algún sistema de seguridad.

El último informe de la CMT (Comisión del Mercado de las Telecomunicaciones), de enero de 2009, señalaba que el parque de líneas móviles en España ya ha superado los 52 millones. Por su parte, las estimaciones más recientes de los analistas sitúan la barrera de usuarios de teléfonos móviles en más de 4.500 millones en todo el mundo para finales de año (es decir, 67 de cada 100 personas tendrán un móvil de aquí a finales de 2009). Esta situación permite vaticinar que es más que probable que el problema de la proliferación de ataques a estos dispositivos vaya aumentando de magnitud con el paso del tiempo.

En cuanto a los daños que estos virus pueden crear en dichos dispositivos son variados y numerosos. Entre ellos, códigos maliciosos que pueden bloquear el móvil y otros que impiden que se recupere su contenido. Incluso, algunos de ellos sirven para robar la información que el usuario tiene y otros tienen la finalidad de expandir spam (o correo basura) a través de mensajes de texto o multimedia. De hecho, los autores del informe Cisco 2009 Midyear Security Report sobre seguridad informática han descrito nuevas tecnologías y métodos inventados por los creadores de virus para móviles. Entre ellas hay que citar la copia de sí mismos en las tarjetas de memoria; la descarga de módulos complementarios desde Internet; las acciones espía; el deterioro de los datos del usuario; o la cancelación de los instrumentos de protección incorporados en el sistema operativo.

Un poco de historia

Si bien ha sido en los últimos años cuando ha proliferado mayor información sobre los ataques de virus dirigidos a los teléfonos móviles y el daño causado por los mismos, la historia se remonta al año 2004 cuando comenzó a sonar el nombre del gusano Cabir, el primer virus dirigido a esta categoría de producto que utilizaba tecnología Bluetooth para propagarse. Otro archivo malintencionado, y conocido, fue Mosquito, un troyano que enviaba mensajes SMS, de coste elevado, desde los teléfonos infectados. Esto supuso el principio de una nueva tendencia en lo que a software malicioso se refiere. Cabir fue enviado por un grupo de creadores de virus de la República Checa y Eslovaquia, mientras que, en la actualidad, y siguiendo la información recogida en un documento elaborado por Kaspersky Lab, las regiones con más cantidad de programas malignos son Rusia, China e Indonesia, entre otros.

El informe "Virus para móviles" realizado por INTECO (Instituto Nacional de Tecnologías de la Información), en 2006, ya señalaba que el crecimiento de la capacidad de los dispositivos móviles para



>>> CONSEJOS PARA NO CONTAGIARTE

Resulta de vital importancia llevar a cabo una serie de pautas si no queremos sufrir uno de estos ataques. Una vez que los terminales se han convertido en dispositivos capaces de conectarse a Internet y a otros equipos, las medidas de seguridad deben extremarse y asemejarse a las que todos los usuarios establecen en sus ordenadores, ya sea el de la empresa o el de uso personal.

Entre las advertencias más comunes destaca desactivar la tecnología Bluetooth si no se necesita utilizar, evitando que el terminal entre en contacto con otro dispositivo y se contagie. Asimismo, si ha de utilizarse esta tecnología inalámbrica, el usuario deberá ir al menú ajustes de Bluetooth y seleccionar "Oculto" en la sección "Visibilidad". Así el teléfono sólo aceptará aquellos dispositivos que hayan sido seleccionados previamente. De igual manera, si la opción "Oculto" no estuviera activada, y algún terminal entrara en contacto con otro, el consejo en este caso es no aceptar ninguna aplicación que proceda de él.

almacenar datos, la posibilidad de sincronizarlos con el ordenador de la oficina o el de casa y la integración del correo electrónico, entre otras características, permitirían desarrollar aplicaciones que hasta la fecha se realizaban normalmente con un PC; todas ellas, acciones que resultarían muy atrayentes para los hackers. Por este motivo, continuaba el informe, los ciberdelincuentes empezarían a tener en cuenta todas estas circunstancias para intentar sacar el mayor provecho de esta situación y multiplicar las posibilidades de riesgo.



Entre ellas, a medida que el número de servicios aumentase, surgirían más posibilidades de encontrar fisuras para la intrusión y el robo, mayores opciones de capturar claves, crecería el número de propagaciones debido a la mayor cantidad de dispositivos móviles, o la difusión de los virus malignos sería más rápida debido a la mayor velocidad de transferencia que se conseguiría. Este estudio concluía que, a los virus existentes en ese momento, le seguirían otros muchos más perniciosos a medida que las características técnicas de los terminales fuesen incrementando.

A la par que dicho informe, en el año 2006 proliferaron unos gusanos de envío masivo de correo (como, por ejemplo, VBS/Eliles.A), que contenían adjuntos malignos y que llevaron a cabo intentos de phishing a los usuarios de los móviles Nokia Serie 60. Posteriormente, tuvo lugar el salto de los virus del ordenador al terminal, como el caso de MSIL/Xrove.a, que utilizaba el lenguaje intermedio de Microsoft (Microsoft Intermediate Language), y que se ejecutaba en numerosos dispositivos. Por otro lado, SymbOS/Mobispy fue el primer malware para móviles que activaba el teléfono infectado de forma remota y que enviaba copias secretas de los mensajes de texto.

Por el contrario, los virus dirigidos a los móviles que existen en la actualidad se asemejan mucho a los virus de PC, es decir, archivos autoejecutables que se camuflan en forma de otro tipo de ficheros o software para expandirse lo más rápidamente posible y provocar el mayor daño.

Ahora, los delincuentes y creadores de malware u otros virus para teléfonos, utilizan la tecnología Bluetooth como sistema de propagación de sus acciones criminales. Y es que el método más rápido que tienen de propagarse es a través de mensajes multimedia, compartiendo juegos, audio, aplicaciones, etc., todos ellos transmitidos de manera inalámbrica. De ahí que la posibilidad de intercambiar archivos mediante esta tecnología u otras, como el Wi-Fi, hace que los dispositivos móviles sean más vulnerables.

Es el caso de la aparición, este año, de Sexy Space. De hecho, Symantec ha alertado de que está proliferando el envío de mensajes de la aplicación Sexy Space, que invita a contenidos para adultos, provocando que el teléfono se convierta en un "zombie" que enviará, a su vez, esos mismos mensajes a toda la lista de contactos del terminal. También se encuentra Sexy View, dirigido a móviles que tienen Symbian como sistema operativo: en este caso, y una vez instalado el malware, enviará un SMS a todos los números de la libreta de direcciones.

>>> AMENAZAS MÓVILES MULTIPLATAFORMAS

El informe sobre programas nocivos para teléfonos móviles "Virología móvil", publicado por Kaspersky Lab, describe algunos de los nuevos métodos de los creadores de virus para móviles. De hecho, casi tres años después de la edición del primer informe, los expertos de la compañía han presenciado cambios importantes en el mundo de estos dispositivos.

Debido a que no existe un líder claro en el mercado de los sistemas operativos para estos dispositivos, los ciberdelincuentes no pueden realizar ataques masivos contra la mayoría de terminales, de ahí que se dediquen a desarrollar amenazas móviles aplicables a multiplataformas. Por ejemplo, el software malicioso Java 2 Micro Edition (J2ME) que asegura la funcionalidad del lenguaje Java en los dispositivos móviles independientemente de la plataforma. De hecho, J2ME funciona en casi todos los teléfonos móviles y smartphone modernos. Este programa maligno J2ME ha llegado a ocupar, durante los tres años que han pasado desde el primer informe de Kaspersky, el segundo lugar entre todos los objetos detectados por la empresa (con un 35%), cediendo el liderazgo a Symbian (con un 49%), el sistema operativo que más ataques sufre al ser el más extendido entre los terminales. Si bien hay que tener en cuenta que al existir varias plataformas para móviles, la propagación de estos virus se ve dificultada. De ahí que quede aún cierto margen de maniobra y de seguridad.



A pesar de que en la actualidad las noticias relacionadas con el phishing (delito cibernético vinculado a las estafas y que tiene a la banca como protagonista), suelen ser bastante habituales, también es necesario hacer un poco de memoria histórica y recordar que nos encontramos ante un tipo de delito que se remonta a 1.996.

A este respecto, cabe citar un estudio de Trend Micro sobre una encuesta hecha a 1.000 personas mayores de edad y usuarios de un smartphone. Ha revelado que únicamente un 23% emplea software de seguridad ya integrado en sus terminales y que un 20% de los mismos dice haberse encontrado con algún fraude relacionado con esta práctica fraudulenta.

Ataques cada vez más comunes

El informe Cisco 2009 Midyear Security Report sobre seguridad informática ha puesto de manifiesto las tendencias más extendidas y los ataques más sofisticados que se producen en la actualidad. Y ha quedado patente que, desde principios de este año, han aparecido dos o tres campañas semanales cuyo objetivo son los móviles.

De hecho, Cisco define el creciente mercado de estos dispositivos como una "nueva frontera de fraude irresistible para los criminales". Con la cantidad antes citada de más de cuatro mil millones de líneas telefónicas móviles en todo el mundo, un delincuente podría lanzar una red muy amplia, incluso si el ataque se produjera sólo sobre una parte de los usuarios.

En esta misma línea, el informe "Virología móvil" de Kaspersky Lab señala que el comportamiento más frecuente de estos programas maliciosos observado, durante los últimos dos años, es el envío de mensajes SMS a través del móvil del usuario, sin que éste lo sepa.

Este tipo de programa se llama troyano-SMS y utiliza métodos de engaño muy sofisticados ya que se propaga cuando se "obliga" al usuario a pulsar el botón y, así, mandar un mensaje a un número determinado. Es lo que el informe Cisco 2009 Midyear Security Report denomina "SMiShing" y consiste en una variante del phishing en el que se emplean mensajes de texto dirigidos, precisamente, a los usuarios de telefonía móvil.

Mientras, el canal más habitual para la difusión de esta clase de programas tipo troyanos son los portales WAP, donde se ofrece la descarga de software de distintos tipos y contenidos multimedia. De hecho, la mayoría de los troyanos-SMS se disfrazan de aplicaciones que ofrecen servicios gratuitos de intercambio de SMS o acceso a Internet; si bien existen algunos que vienen ocultos en forma de mensajes multimedia.



Estamos ante lo que puede ser considerado como un nuevo caballo de batalla para las empresas de desarrollo de sistemas operativos para móviles, que verán abierto un nuevo frente contra el que luchar para poder capacitar a sus entornos de una mayor seguridad. Sobre todo si tenemos en cuenta que los ciberdelincuentes buscan siempre nuevas formas para llevar a cabo sus delitos.





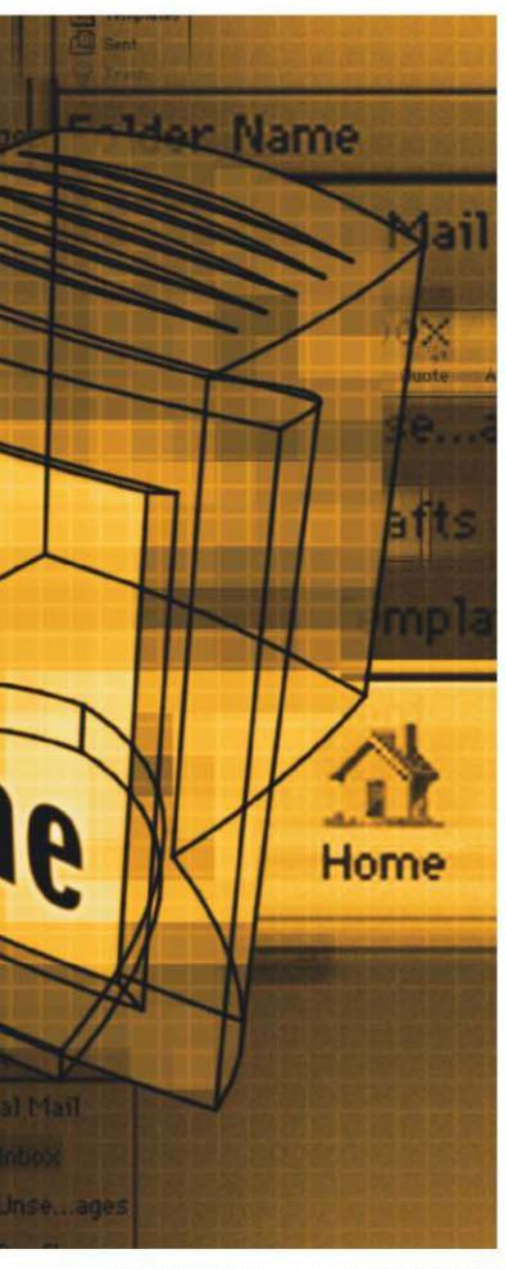
Banda ancha, vídeos en streaming

La última tendencia para el visionado de todo tipo de contenidos de vídeo en Internet es el streaming, una tecnología que permite disfrutar de los archivos sin descargarlos al ordenador.

Desde la generalización de la banda ancha, la oferta de contenidos multimedia en Internet se ha multiplicado. Y es que, con conexiones que alcanzan varios megas de velocidad, la descarga de grandes archivos resulta muy rápida. Un nuevo sistema está desbancando a este modo de acceder a los contenidos. Se trata del streaming, una tecnología multimedia que permite visualizar vídeos directamente desde una página web o desde un software reproductor, sin necesidad de descargar primero los archivos en el ordenador. Los contenidos disponibles con este sistema abarcan desde programas en directo (live), cuando la transmisión se realiza a la vez que la emisión, hasta los conocidos como bajo demanda (on demand), método que permite que los visitantes elijan cuándo ver un vídeo. Posiblemente, entre los eventos más buscados destaquen los deportivos pero, además, el streaming se ha convertido en uno de los modos preferidos por los internautas para ver películas y series de televisión.

Todo beneficios

El éxito de esta tecnología multimedia está directamente relacionado con los beneficios que proporciona al usuario. El primero y más evidente es que, como los vídeos están alojados en un servidor, la capacidad del disco duro permanece intacta para dedicarla a otros usos.



YOUTUBE

Fundada en 2005, es la comunidad de vídeos on demand por excelencia. Los datos hablan por sí solos: cada minuto, los millones de usuarios de Youtube cargan unas 20 horas de imagen en movimiento, que suman cientos de miles de archivos nuevos al día. Y las visitas son aún mayores ya que, diariamente, se reproducen cientos de millones. Su versatilidad es clara, porque lejos de limitarse a la página web, también se ha adaptado a otros soportes como los dispositivos móviles y, además, permite que sus vídeos se visualicen desde otras páginas y sitios. El portal ofrece a sus visitantes la posibilidad de registrarse, con lo que podrán subir y compartir contenidos fácilmente, guardar sus favoritos, crear listas de reproducción, poner comentarios y valorar las aportaciones de otros usuarios.





YouTube™





Además, una vez se ha decidido qué ver y se ha localizado el archivo, la visualización es instantánea, ya que no hay que esperar a que el vídeo se descargue por completo al ordenador. En el peor de los casos, si la conexión es lenta, la reproducción tardará unos segundos en comenzar. Cuando se trata de eventos en vivo, los beneficios son todavía mayores, ya que se sintonizan programas internacionales y otros que en España emiten canales de pago. Por último, destacar que casi la totalidad de las páginas y programas que ofrecen streaming de vídeo son gratuitos, aunque algunos requieren un registro previo.

Página web *www.youtube.com*

USTREAM

Es una página de streaming en directo, así que todos los programas que emite lo hacen en tiempo real. Su principal pretensión es convertirse en el sitio de referencia para todos aquellos que quieren retransmitir episodios de su propia vida. A estos internautas, las emisiones les dan derecho a tener una página personal desde la que centralizar todos sus vídeos. Aun así, el atractivo para los internautas es su espacio de retransmisiones televisivas y, sobre todo, las deportivas. La forma de facilitar una localización óptima de los eventos es organizarlos por secciones. Junto a los contenidos, aparece un chat con el que cambiar impresiones con el resto de usuarios. Una última opción es colocar enlaces de UStream en cualquier web o red social, como Youtube, para que los vídeos aparezcan en los dos portales. Para utilizarlo (tanto ver como cargar archivos), hay que registrarse.





Página web *www.ustream.tv*

MEGAVIDEO

Los creadores de Megaupload, uno de los sitios más populares para cargar archivos y compartirlos on line con otros usuarios, han desarrollado también su herramienta para visualizar vídeos. No es necesario registrarse para hacerlo aunque, como consecuencia, no se puede estar conectado al servicio más de 72 minutos seguidos. Al sobrepasar esta cifra, hay que esperar otros 54 minutos antes de retomar la reproducción (si no se conocen los trucos que circulan por Internet, que ayudan a saltarse estas restricciones). Para cargar archivos hay que estar registrado. El servicio también ofrece una cuenta Premium con algunas ventajas más. Los contenidos están divididos en categorías como los más populares, los más vistos, por duración o por su temática. Su reproductor tiene las funciones básicas, incorpora elementos para la gestión, algunos datos de interés, puntuación, información sobre el autor...





Página web *www.megavideo.com*

TVU PLAYER

Este es un ejemplo representativo de que también hay programas especialmente pensados para el streaming de vídeo. TVU Player ofrece una interfaz muy intuitiva que distribuye las emisiones por lengua o área temática y permite crear listas de reproducción y de favoritos. Está asociado a TVUnetworks, una página web que integra un directorio con canales de televisión de todo el mundo y la programación que cada día estará disponible para los usuarios. Además, el registro ofrece la posibilidad de interactuar con el resto de internautas, y añadir y compartir canales.

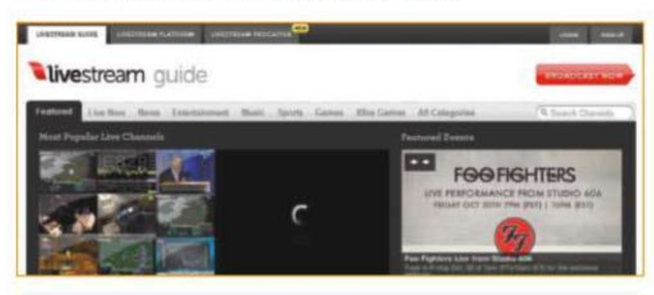




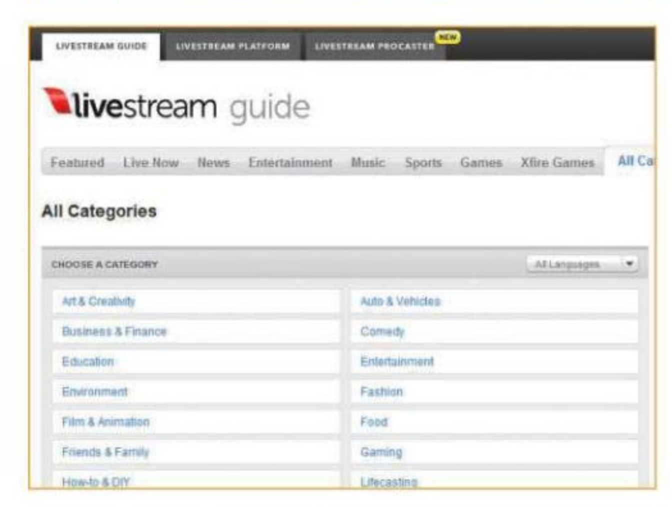
Página web *www.tvunetworks.com*

LIVESTREAM

Con oferta de contenidos on demand y en vivo, integra un programa de visualización totalmente personalizable (ofrece diversas plantillas) para que se adapte a la apariencia de un sitio web. A la vez que se ven los vídeos, se puede chatear en el área destinada para ello. Las opciones de integración son muy amplias: en Twitter, el estado cambia automáticamente con el nombre del vídeo que se está viendo en ese momento. Una de sus prestaciones más atractivas es el servicio gratuito Procaster, que permite gestionar los streamings directamente desde el ordenador, sin tener que recurrir al navegador.





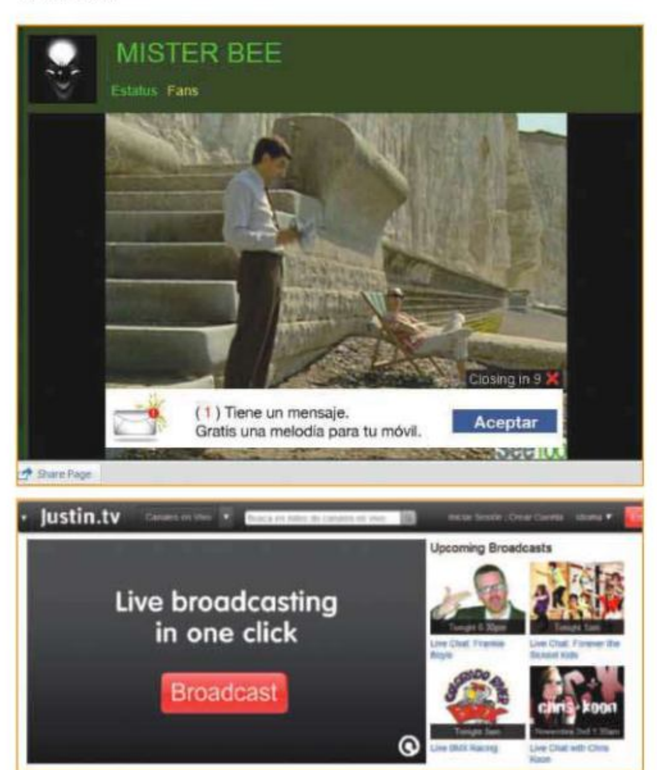


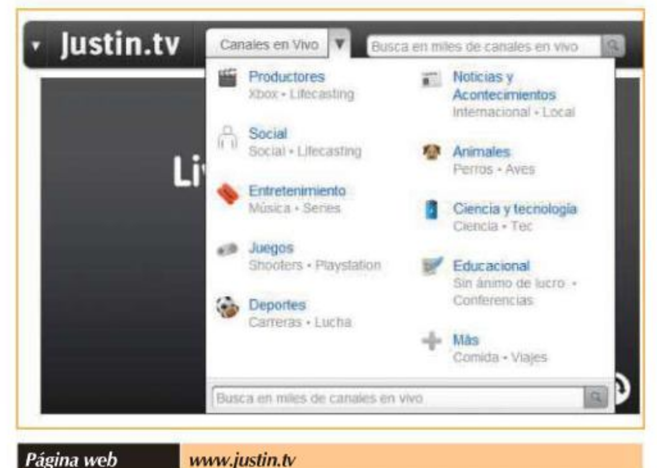


Página web *http://livestream.com*

JUSTIN.TV

Esta comunidad virtual para transmitir y ver vídeos presume de ser líder en este tipo de webs, con más de 41 millones de visitas únicas al mes y un número de canales en emisión superior a los 500.000. Sus contenidos on demand y en vivo están distribuidos por temáticas. Como permite integrar su reproductor en diversos sitios de redes sociales y blogs, si se sincroniza con Twitter se envía un tweet al ver un vídeo, y lo mismo ocurre con MySpace, que actualizará automáticamente el estado.





Página web *www.justin.tv*

Uno de los conceptos más básicos sobre la arquitectura de los computadores actuales es, a su vez, uno de los conceptos menos conocidos y -sobre todo- menos comprendidos por los usuarios de ordenadores. Spoiler alert: la memoria es volátil. Los datos que hay en memoria se pierden irremisiblemente al apagar nuestros ordenadores. Sin embargo, no hace falta que congeléis vuestras memorias para mantener dichos datos... porque para eso se inventó la memoria persistente.



jWadalPasswd (V)

Hola a todos, queridos lectores, y bienvenidos una vez más al Curso de Java Útil. Estoy seguro que la gran mayoría de vosotros seréis conscientes de la circunstancia comentada en la introducción del artículo. Como sabréis, la memoria principal o memoria RAM, uno de los elementos principales en la arquitectura de Von Neumann (o, como debería denominarse siendo más correctos, arquitectura de Eckert-Mauchly), es volátil.

La mala memoria de la memoria

Dejando a un lado recientes investigaciones científicas que involucran el análisis forense y el manejo de nitrógeno líquido -disciplinas complejas y peligrosas respectivamente-, los datos contenidos en la memoria RAM desaparecen si no se "refrescan" con una cierta frecuencia, lo cual requiere de alimentación eléctrica. Como consecuencia, apagar el ordenador ocasiona que todos nuestros datos pasen a desaparecer en el limbo informático.

Por supuesto, si cada vez que apagáramos el ordenador perdiéramos absolutamente todos nuestros datos, estos cacharros no serían demasiado útiles para las personas. Pensad, por ejemplo, en toda la información contenida en Internet. Aunque sólo consideráramos el 1% que no es pornografía, estamos hablando de cantidades ingentes de datos que no queremos perder. Por supuesto, tampoco el 99% restante. :-P

Para paliar este problema existen los denominados sistemas de almacenamiento secundarios (en contraposición a la memoria principal o memoria RAM) que, en este caso sí, son sistemas persistentes que almacenan la información a perpetuidad, al menos en principio. Si obviamos los aspectos relacionados con el deterioro físico de los medios, o la evolución de los nuevos soportes, que no resultan relevantes para los objetivos de este curso, podemos afirmar que la información lógica almacenada en un sistema de almacenamiento persistente estará allí por los siglos de los siglos.

Nuestro particular Diógenes informático

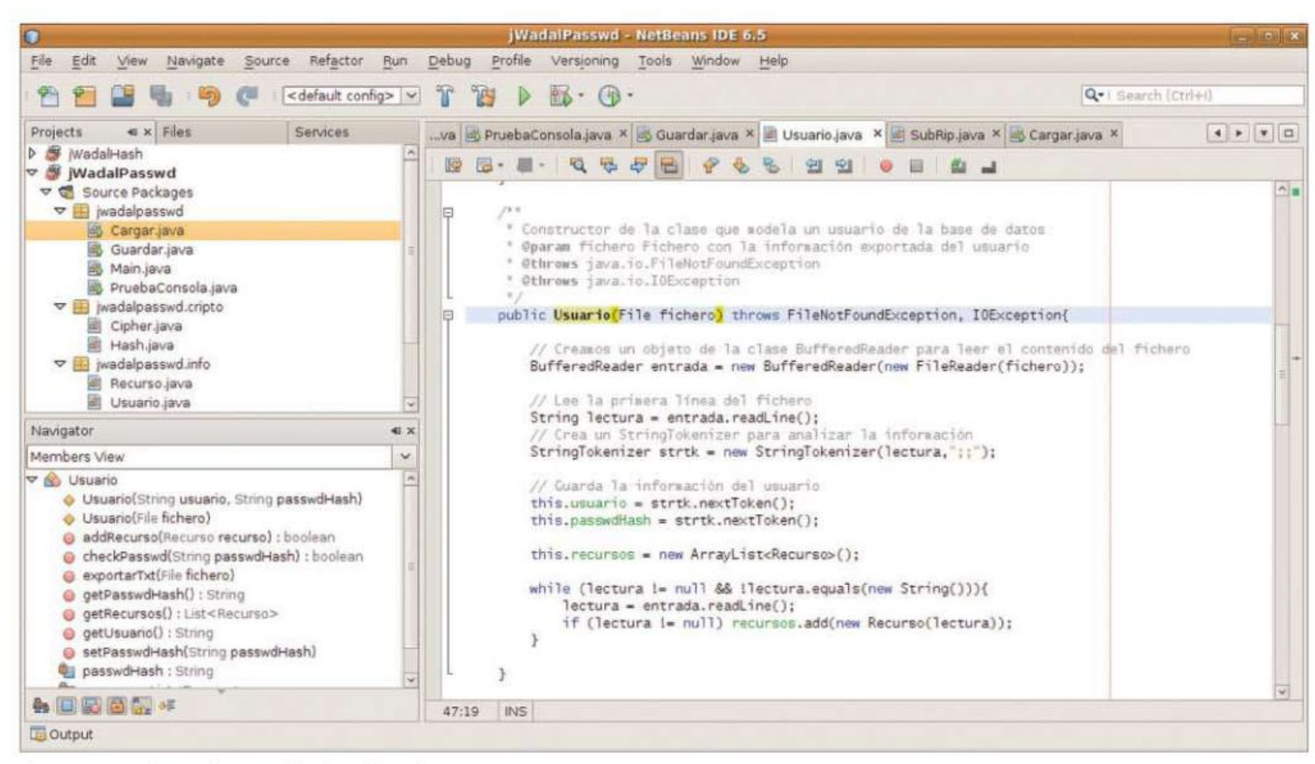
En el caso de nuestro programa jWadalPasswd, nos interesa tener la capacidad de guardar los datos que introduzcamos, por lo que debemos implementar algún mecanismo de almacenamiento en memoria secundaria. Para empezar, y para evitar estar introduciendo una y otra vez datos de prueba, vamos a automatizar dicha tarea en una nueva clase de tipo Main que llamaremos "Guardar.java". El código del método "main" será el siguiente:

```
/**
  * @param args the command line
arguments
  */
public static void main(String[]
args){

   // Crea el usuario
   String nombreUsuario =
"Ramiro";
   String password = "@rroba";
   Usuario usuario = new Usuario(n
ombreUsuario,Hash.getHashWhirlpool
(password));

   // Crea el primer recurso
   HashMap params = new HashMap();
   params.put("localizacion","http
://www.google.es/");
   params.put("identificador","rami
ro");
   params.put("password","contrase
ña");
   params.put("informacion","Cuent
a de correo electrónico");

   Recurso recurso = null;
   try {
```



Constructor alternativo para la clase Usuario.

```
    recurso = new
Recurso(params,Hash.
getHashMD5(password));
    } catch (DataLengthException
ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    } catch (IllegalStateException
ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    } catch
(InvalidCipherTextException ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    }

  usuario.addRecurso(recurso);

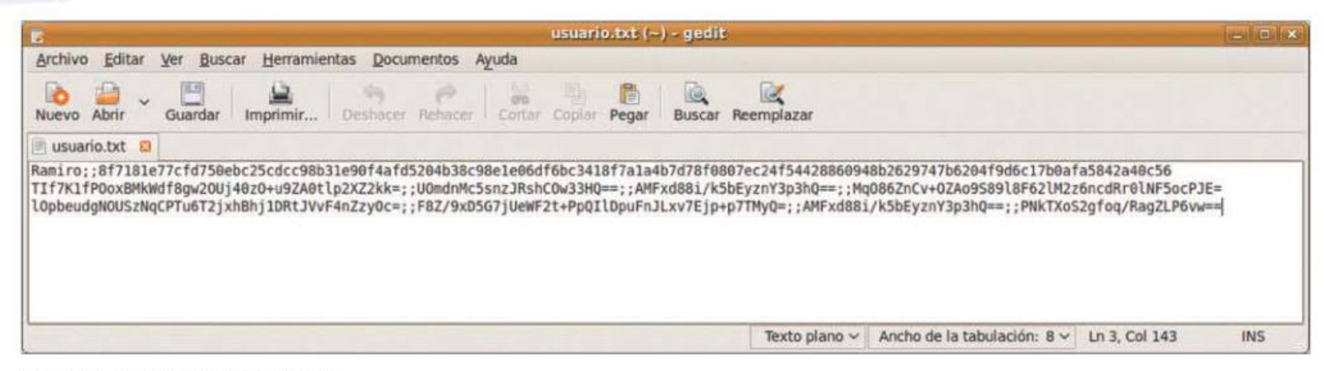
  // Crea el segundo recuso
  params = new HashMap();
  params.put("localizacion","http
://www.hotmail.com/");
  params.put("identificador","rami
ro@hotmail.com");
  params.put("password","contrase
ña");
  params.put("informacion","-");
```

```
  try {
    recurso = new
Recurso(params,Hash.
getHashMD5(password));
    } catch (DataLengthException
ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    } catch (IllegalStateException
ex) {
    Logger.getLogger(Guardar.class.
getName()).log(Level.SEVERE, null,
ex);
    } catch
(InvalidCipherTextException ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    }

  usuario.addRecurso(recurso);

  // Comprueba que se han añadido
los recursos
  List<Recurso> recursos =
usuario.getRecursos();
  if (recursos.size() < 1){
    System.out.println("¡No hay
recursos!");
  }
```

```
  for (Recurso r:recursos){
  try {
    System.out.println();
    System.out.
println("Localización: "
+ r.getLocalizacion(Hash.
getHashMD5(password)));
    System.out.
println("Identificador: "
+ r.getIdentificador(Hash.
getHashMD5(password)));
    System.out.println("Password:
" + r.getPassword(Hash.
getHashMD5(password)));
    System.out.
println("Información adicional:
" + r.getInformacion(Hash.
getHashMD5(password)));
    } catch (DataLengthException
ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    } catch (IllegalStateException
ex) {
    Logger.getLogger(Guardar.
class.getName()).log(Level.SEVERE,
null, ex);
    } catch
(InvalidCipherTextException ex) {
    Logger.getLogger(Guardar.
```



Exportando la información cifrada.

```
class.getName()).log(Level.SEVERE,
null, ex);
     }
   }
   System.out.println();

}
```

Cuando lo ejecutemos, obtendremos la siguiente salida:

```
init:
deps-jar:
compile-single:
run-single:

Localización: http://www.google.es/
Identificador: ramiro
Password: contraseña
Información adicional: Cuenta de
correo electrónico

Localización: http://www.hotmail.
com/
Identificador: ramiro@hotmail.com
Password: contraseña
Información adicional: -

BUILD SUCCESSFUL (total time: 0
seconds)
```

Bien, parece que todo funciona correctamente.

Guardando a un fichero

Ya estamos en condiciones de guardar la información cifrada generada por nuestro programa, para su posterior recuperación en una ejecución posterior. ¿Y cómo guardar dicha información en un fichero? La primera idea que acude a nuestra mente en estos casos suele ser un fichero de texto. Como ya sabemos más o menos cómo funciona este proceso, gracias a lo que aprendimos con jWadalSubs, vamos a implementar un sencillo sistema de exportación de datos.

Lo primero que haremos será idear un código de representación como cadena de texto de nuestros recursos cifrados. Ya poseemos la información cifrada de cada atributo representada como una cadena de texto codificada en Base64, por lo que sólo necesitamos unir toda la información del recurso en una única cadena. Una forma de hacerlo, por poner un ejemplo, es seguir la siguiente estructura:

```
campo1;;campo2;;campo3;;...
```

La idea es la misma que subyace a los ficheros CSV (Comma-Separated Values), separando la información mediante unos delimitadores especiales, que indican el comienzo de un nuevo campo. En nuestro caso, vamos a utilizar un doble punto y coma como delimitador, por ser una concurrencia de caracteres que no se da en ningún caso en el lenguaje natural, ni en la codificación Base64. Esta estructura nos permitirá posteriormente recuperar la información de una forma mucho más sencilla, mediante la utilización de la clase StringTokenizer.

Ahora necesitamos representar la información de un recurso como una única cadena de texto. Para ello, Java suele utilizar un método que es común a todos los objetos del lenguaje (pues se define en la propia clase Object), y que se denomina "toString()". Para indicar al compilador que deseamos sobrescribir el método heredado de clases superiores en la jerarquía, debemos utilizar el modificador "@Override" en la declaración del método.

De esta forma, crearemos el siguiente método en la clase "Recurso":

```
/**
  * Devuelve la representación
como cadena del recurso
  * @return Representación como
cadena del recurso
  */
@Override
public String toString(){
    return (
      this.localizacion + ";;" +
      this.identificador + ";;" +
      this.password + ";;" +
      this.informacion
      );
}
```

Ahora, y en la clase "Usuario", debemos definir un método para exportar toda la información del usuario a un único fichero. Esta información comprende tanto el nombre de usuario y el hash Whirlpool de la contraseña (que exportaremos usando el mismo método que en el caso de los recursos), así como la información de cada uno de los recursos asociados al usuario. El método será como sigue:

```
/**
  * Exporta la información de un
usuario a un fichero de texto
  * @param fichero Fichero donde
se almacenará la información del
usuario
  * @throws java.
io.FileNotFoundException
  */
public void exportarTxt(File
fichero) throws
FileNotFoundException{

  // Creamos un objeto de la
clase PrintWriter para escribir el
fichero
  PrintWriter salida = new
PrintWriter(fichero);
```

```
    // Guarda la información del
usuario
    salida.println(usuario + ";;" +
passwdHash);

    // Guarda cada uno de los
recursos
    for (Recurso r:recursos){
    salida.println(r.toString());
   }

    // Cerramos el flujo del fichero
    salida.close();

}
```

Por último, vamos a añadir unas líneas al final del método "main" de la clase "Guardar", para que se guarde la información del usuario a un fichero arbitrario:

```
File fichero = new File("/home/
ramiro/usuario.txt");
try {
    usuario.exportarTxt(fichero);
} catch (FileNotFoundException ex)
{
    Logger.getLogger(Guardar.class.
getName()).log(Level.SEVERE, null,
ex);
}
```

```
System.out.println("Información
guardada correctamente en: " +
fichero.toString());
```

Cuando ejecutemos la clase "Guardar" en esta ocasión, obtendremos la siguiente saldia:

```
init:
deps-jar:
compile-single:
run-single:

Localización: http://www.google.es/
Identificador: ramiro
Password: contraseña
Información adicional: Cuenta de
correo electrónico

Localización: http://www.hotmail.com/
Identificador: ramiro@hotmail.com
Password: contraseña
Información adicional: -

Información guardada correctamente
en: /home/ramiro/usuario.txt
BUILD SUCCESSFUL (total time: 0
seconds)
```

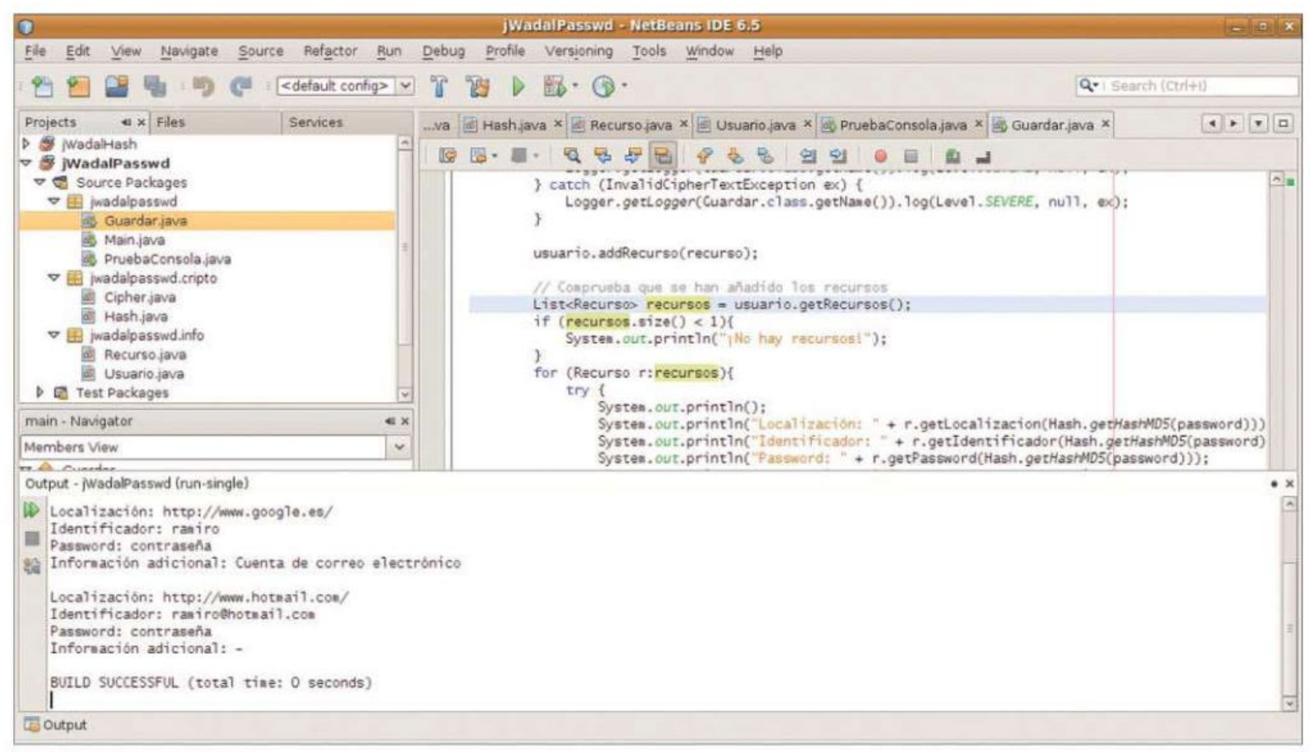
Por último, si accedemos al fichero generado, encontraremos la siguiente información:


```
Ramiro;;8f7181e77cfd750ebc25cdcc98
b31e90f4afd5204b38c98e1e06df6bc34
18f7a1a4b7d78f0807ec24f5442886094
8b2629747b6204f9d6c17b0afa5842a40
c56
TIf7K1fPOoxBMkWdf8gw2OUj40zO+u9ZA0
tlp2XZ2kk=;;UOmdnMc5snzJRshCOw33HQ
==;;AMFxd88i/k5bEyznY3p3hQ==;;MqO
86ZnCv+OZAo9S8918F621M2z6ncdRr01NF
5ocPJE=
lOpbeudgNOUSzNqCPTu6T2jxhBhj1DRt
JVvF4nZzyOc=;; F8Z/
9xD5G7jUeWF2t+PpQIlDpuFnJLxv7Ejp
+p7TMyQ=;; AMFxd88i/
k5bEyznY3p3hQ==;; PNkTXoS2gfoq/
RagZLP6vw==
```


Recuperando la información

Por supuesto, de nada sirve exportar la información si luego no la importamos. Vamos pues a recuperar la información que acabamos de exportar. El primer problema que nos encontramos es que, en esta ocasión, no podemos definir un método para importar la información de un usuario dentro de la propia clase "Usuario".

Esto es así debido a que, para poder invocar un método de un objeto, necesitamos primero haberlo instanciado. Y no podemos



Nuestro banco de pruebas.

instanciar un nuevo usuario en nuestro sistema si no disponemos del nombre de usuario y la contraseña. Como dichos datos se encuentran a su vez en el fichero de exportación, tenemos que hacer algo nuevo.

Lo que vamos a hacer, dado que queremos crear el nuevo usuario en base a la información guardada en el fichero de texto, es definir un nuevo método constructor. Para ello, vamos a hacer uso de la capacidad de sobrecarga de operadores que la orientación a objetos -y, por tanto, Java- nos brinda. La sobrecarga de operadores permite definir, utilizando un mismo nombre, métodos diferentes en base a los distintos parámetros recibidos. En este caso, ya existe un método constructor que recibe como parámetros un HashMap y un String, y vamos a definir uno nuevo que recibe como parámetro un fichero.

El código será el siguiente:

```
/**
  * Constructor de la clase que
modela un usuario de la base de
datos
  * @param fichero Fichero con la
información exportada del usuario
  * @throws java.
io.FileNotFoundException
  * @throws java.io.IOException
  */
public Usuario(File fichero)
throws FileNotFoundException,
IOException{

   // Creamos un objeto de la
clase BufferedReader para leer el
contenido del fichero
   BufferedReader entrada
= new BufferedReader(new
FileReader(fichero));

   // Lee la primera línea del
fichero
   String lectura = entrada.
readLine();
   // Crea un StringTokenizer para
analizar la información
   StringTokenizer strtk = new
StringTokenizer(lectura,";;");

   // Guarda la información del
usuario
   this.usuario = strtk.
nextToken();
   this.passwdHash = strtk.
nextToken();

   this.recursos = new
ArrayList<Recurso>();

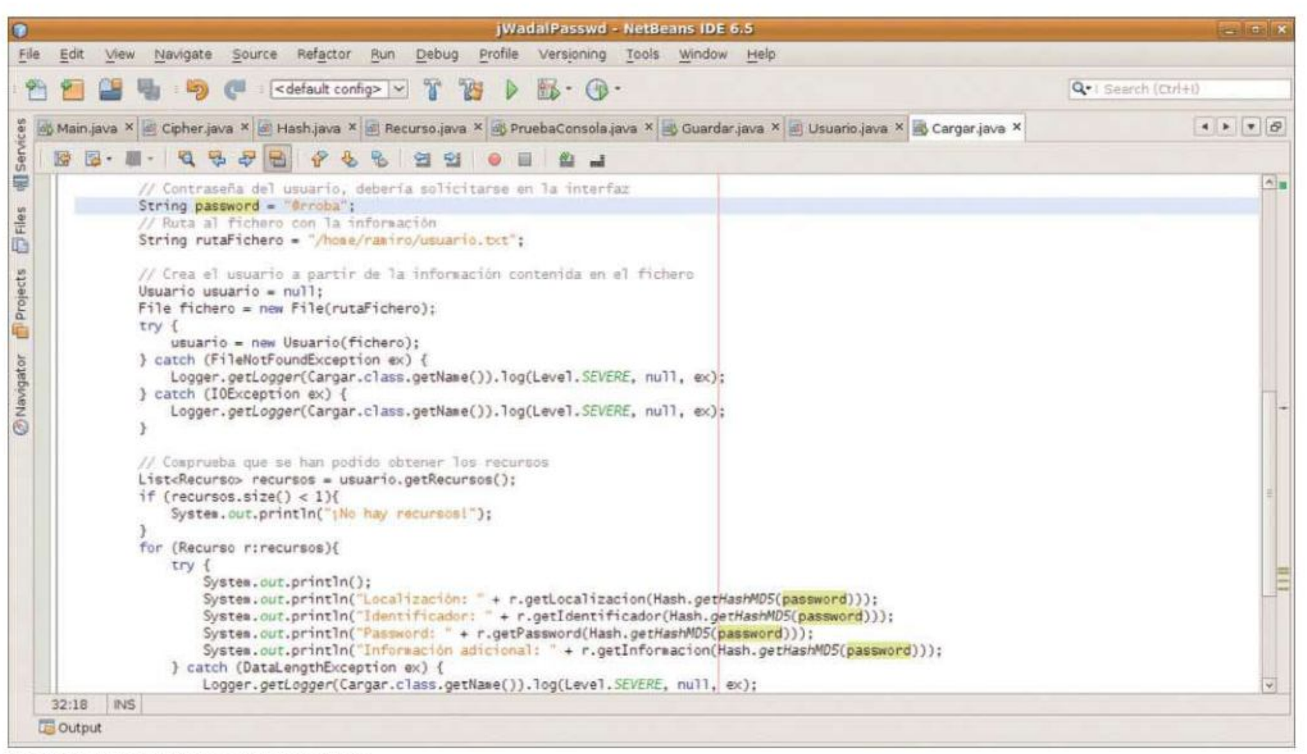
   while (lectura != null &&
!lectura.equals(new String())){
      lectura = entrada.readLine();
      if (lectura != null) recursos.
add(new Recurso(lectura));
   }

}
```

Como podéis comprobar, este constructor hace uso a su vez de un constructor de la clase "Recurso" que aún no existe. Al igual que en el caso de la clase "Usuario", vamos a definir un nuevo constructor sobrecargado que lea la información de una cadena de texto codificada con nuestro particular sistema.

El nuevo constructor de la clase "Recurso" será como sigue:

```
/**
  * Constructor de la clase que
modela un recurso de la base de
datos
  * @param cadenaImportada Cadena
importada con los datos cifrados
del recurso
  */
```



Recuperando la información exportada.

```
public Recurso(String
cadenaImportada){

   // Crea un StringTokenizer para
analizar la información
   StringTokenizer strtk = new
StringTokenizer(cadenaImportada,";
;");

   // Guarda la información del
recurso
   this.localizacion = strtk.
nextToken();
   this.identificador = strtk.
nextToken();
   this.password = strtk.
nextToken();
   this.informacion = strtk.
nextToken();

}
```

Una vez codificados los nuevos métodos constructores, estamos en condiciones de crear una nueva clase de tipo Main "Cargar" para recuperar la información del fichero de texto. El código será el siguiente:

```
/**
  * @param args the command line
arguments
  */
public static void main(String[]
args) {

   // Contraseña del usuario,
debería solicitarse en la interfaz
   String password = "@rroba";
   // Ruta al fichero con la
información
    String rutaFichero = "/home/
ramiro/usuario.txt";

   // Crea el usuario a partir
de la información contenida en el
fichero
   Usuario usuario = null;
   File fichero = new
File(rutaFichero);
   try {
    usuario = new Usuario(fichero);
  }  catch  (FileNotFoundException
ex) {
   Logger.getLogger(Cargar.class.
getName()).log(Level.SEVERE,  null,
ex);
   } catch (IOException ex) {
    Logger.getLogger(Cargar.class.
getName()).log(Level.SEVERE,null,ex);
  }

  // Comprueba que se han podido
obtener los recursos
  List<Recurso> recursos =
usuario.getRecursos();
  if (recursos.size() < 1){
    System.out.println("¡No hay
recursos!");
  }
  for (Recurso r:recursos){
   try {
    System.out.println();
    System.out.
println("Localización: "
+ r.getLocalizacion(Hash.
getHashMD5(password)));
    System.out.
println("Identificador: "
+ r.getIdentificador(Hash.
getHashMD5(password)));
    System.out.println("Password:
" + r.getPassword(Hash.
getHashMD5(password)));
    System.out.
println("Información adicional:
" + r.getInformacion(Hash.
getHashMD5(password)));
    } catch (DataLengthException ex) {
    Logger.getLogger(Cargar.class.
getName()).log(Level.SEVERE,null,ex);
    } catch  (IllegalStateException
ex)  {
    Logger.getLogger(Cargar.class.
getName()).log(Level.SEVERE,null,ex);
    } catch
(InvalidCipherTextException ex)  {
    Logger.getLogger(Cargar.class.
getName()).log(Level.SEVERE,  null,
ex);
    }
  }
  System.out.println();

}
```

Al ejecutar este método, obtendremos la siguiente salida:

```
init:
deps-jar:
compile-single:
run-single:

Localización: http://www.google.es/
Identificador: ramiro
Password: contraseña
Información adicional: Cuenta de
correo electrónico

Localización: http://www.hotmail.com/
Identificador: ramiro@hotmail.com
Password: contraseña
Información adicional: -

BUILD SUCCESSFUL (total time: 0
seconds)
```

Parece que todo funciona correctamente. :-)

El mes que viene

Este mes hemos construido un sistema de exportación e importación de datos para nuestro programa, de forma que ya no resulta necesario introducir la información cada vez que lo ejecutamos. Para ello, hemos utilizado como base ficheros de texto, codificando la información mediante un sistema que nos permite recuperarla fácilmente haciendo uso de los StringTokenizer. Según las pruebas realizadas, el sistema funciona correctamente en ambos sentidos.

No obstante, este sistema no es óptimo, pues adolece de varios problemas: ¿qué pasa si modificamos la estructura de un recurso, añadiendo o eliminando atributos? ¿y si modificamos la información de un usuario? Además, hemos obviado de forma prácticamente completa el sistema de comprobación de errores, y una leve modificación en el fichero de texto podría ocasionar errores en la ejecución del software.

El mes que viene vamos a ver una alternativa para realizar la importación y exportación de los datos de una forma más eficaz, usando la serialización de objetos de Java. Si os sentís con ánimo, podéis buscar información por Internet e intentarlo por vuestra cuenta.

Un mes más, os recuerdo que en mi blog podréis encontrar el código fuente del curso completo, y que mi correo electrónico está a vuestra disposición para que compartáis conmigo dudas, sugerencias y preguntas acerca del desarrollo de los artículos.

¡Hasta el mes que viene!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/

Para bien o para mal, hace bastante tiempo que el desarrollo de software dejó de ser una tarea artesanal. Actualmente, la disciplina de Ingeniería del Software está omnipresente en cualquier desarrollo de tamaño mediano; y no hablemos ya de los grandes proyectos, donde toma prácticamente el papel protagonista. Desde el punto de vista del programador, una de las herramientas más útiles para desarrollar código junto a otros componentes de un equipo, es el sistema de control de versiones.

Implantación de un servidor Subversion

Mejorar el desarrollo concurrente de código

Bienvenidos, queridos lectores. Si alguna vez habéis tenido que trabajar con otras personas en el desarrollo de un mismo código, cosa altamente probable, coincidiréis conmigo en que la sincronización es posiblemente uno de los elementos más problemáticos. Y el problema ya no es tanto cuál es la última versión, cosa que es fácilmente determinable por la fecha de modificación que marca el sistema de ficheros; sino qué se ha añadido o quitado, quién lo ha hecho, y qué había antes en su lugar.

Control de versiones

Para solucionar esta problemática surgen los denominados sistemas de control de versiones. Estos sistemas son los encargados de gestionar todos los elementos almacenados en su interior, y que no tienen por qué limitarse únicamente a código fuente. Además de almacenarlos, se encargan de guardar la información de todos los cambios efectuados sobre un determinado elemento, con información adicional como la fecha o el autor de la modificación; así como de gestionar el acceso a un mismo elemento por parte de varias personas, encargándose automáticamente de la sincronización de todos los cambios, en el caso de que no existan modificaciones sobre las mismas secciones del elemento.

Así, estos sistemas permiten que varias personas trabajen sobre un mismo fichero de código de forma independiente. Al enviar los cambios, el software se encargará de mezclar las diferencias introducidas por cada uno de los programadores, obteniendo una versión global y completa a partir de las modificaciones parciales. Además, permite revisar el historial completo de cambios, siendo posible revertir un determinado fichero al estado en el que se encontraba en cualquier punto de su desarrollo.

Desde el nacimiento de CVS (Concurrent Versions System) allá por 1990, han pasado casi dos décadas, y los sistemas de control de versiones han evolucionado con el tiempo. Actualmente, y además de los clásicos sistemas centralizados (como CVS o el propio Subversion), han surgido nuevos sistemas descentralizados (como GIT o Mercurial), que permiten flexibilizar aún más el trabajo concurrente de varios desarrolladores.

En el número 124 de la revista @rroba hablamos sobre CVS, y vimos cómo desplegar un servidor CVSNT bajo un entorno Microsoft Windows. Sin embargo, CVS tiene ciertas limitaciones, como la imposibilidad de tratar correctamente los ficheros binarios, por lo que surgieron alternativas a éste.

Subversion

El sistema Subversion (comúnmente abreviado como SVN) surge en 1999 como un software diseñado específicamente para sustituir al vetusto CVS. El software, implementado en lenguaje de programación C y distribuido bajo licencia libre Apache, se encuentra actualmente en su versión 1.6.1.

Entre las principales ventajas de Subversion encontramos la atomicidad de las modificaciones sobre los ficheros, la gestión en tiempo constante de ramas y etiquetas, mejor gestión de la comunicación al enviar únicamente las diferencias a los clientes, soporte para WebDAV, posibilidad de manejar correctamente ficheros binarios, etc.

Así pues, vamos a desplegar un servidor Subversion bajo un sistema Ubuntu GNU/Linux 9.04. Además, y aprovechando el soporte que Subversion ofrece para WebDAV, vamos a configurar el acceso al sistema de control de versiones a través del protocolo HTTP, mediante un servidor Web Apache. ¡Manos a la obra!

Trabajando con Subversión.

Preparando el sistema

Lo primero que haremos será instalar el servidor Web Apache. Una instalación básica será suficiente para lo que necesitaremos.

```
ramiro@ubuntu:~$ sudo apt-get
install apache2
Leyendo lista de paquetes...
Hecho
Creando árbol de dependencias
Leyendo la información de
estado... Hecho
Se instalarán los siguientes
paquetes extras:
 apache2-mpm-worker apache2-
utils apache2.2-common libapr1
libaprutil1 libmysqlclient15off
libpq5 mysql-common
Paquetes sugeridos:
 apache2-doc apache2-suexec
apache2-suexec-custom
Se instalarán los siguientes
paquetes NUEVOS:
 apache2 apache2-mpm-worker
apache2-utils apache2.2-
common libapr1 libaprutil1
libmysqlclient15off libpq5 mysql-
common
0 actualizados, 9 se instalarán,
0 para eliminar y 0 no
actualizados.
Necesito descargar 3615kB de
archivos.
Se utilizarán 10,3MB de espacio
de disco adicional después de
esta operación.
¿Desea continuar [S/n]? s
[...]
```

Cuando haya finalizado la instalación de los paquetes, observaremos que se activarán los módulos por defecto del servidor.

```
Enabling site default.
Enabling module alias.
Enabling module autoindex.
Enabling module dir.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module status.
Enabling module auth_basic.
Enabling module deflate.
Enabling module authz_default.
Enabling module authz_user.
Enabling module authz_groupfile.
Enabling module authn_file.
Enabling module authz_host.
```

A continuación, instalaremos el software Subversion desde los repositorios de Ubuntu.

```
ramiro@ubuntu:~$ sudo apt-get
install subversion
Leyendo lista de paquetes...
Hecho
Creando árbol de dependencias
Leyendo la información de
estado... Hecho
```

Se instalarán los siguientes paquetes extras:

```
 libneon27-gnutls libsvn1
Paquetes sugeridos:
 subversion-tools db4.6-util patch
Se instalarán los siguientes
paquetes NUEVOS:
 libneon27-gnutls libsvn1
subversion
0 actualizados, 3 se instalarán,
0 para eliminar y 0 no
actualizados.
```

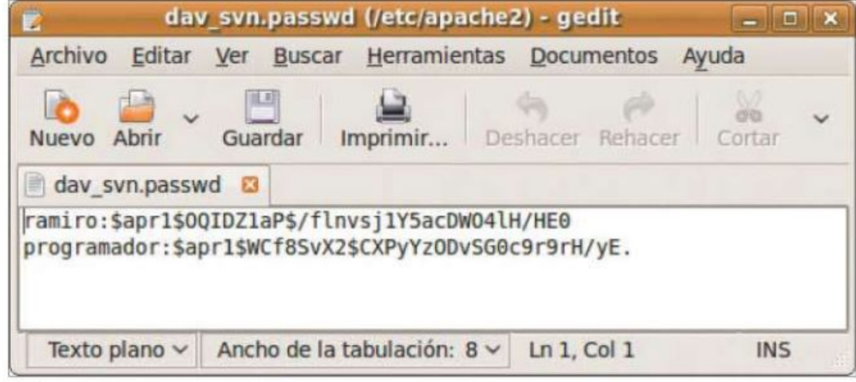
```
Necesito descargar 1189kB de
archivos.
Se utilizarán 6242kB de espacio
de disco adicional después de
esta operación.
¿Desea continuar [S/n]? s
[...]
```

Por último, vamos a instalar el módulo de apache para SVN, llamado "libapache2-svn".

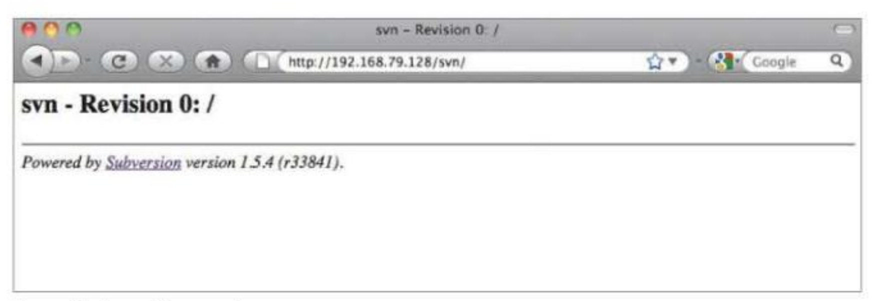
```
ramiro@ubuntu:~$ sudo apt-get
install libapache2-svn
Leyendo lista de paquetes...
Hecho
Creando árbol de dependencias
Leyendo la información de
estado... Hecho
Paquetes sugeridos:
 db4.6-util
Se instalarán los siguientes
paquetes NUEVOS:
 libapache2-svn
0 actualizados, 1 se instalarán,
0 para eliminar y 0 no
actualizados.
Necesito descargar 148kB de
archivos.
Se utilizarán 360kB de espacio de
disco adicional después de esta
operación.
Des:1 ftp://softlibre.unizar.
es jaunty-updates/universe
libapache2-svn 1.5.4dfsg1-
1ubuntu2.1 [148kB]
Descargados 148kB en 4s
(36,9kB/s)
Seleccionando el paquete
libapache2-svn previamente no
seleccionado.
(Leyendo la base de datos ...
107882 ficheros y directorios
instalados actualmente.)
Desempaquetando libapache2-
svn (de .../libapache2-svn_
1.5.4dfsg1-1ubuntu2.1_i386.deb)
...
Configurando libapache2-svn
(1.5.4dfsg1-1ubuntu2.1)...
Considering dependency dav for
dav_svn:
Enabling module dav.
Enabling module dav_svn.
Run '/etc/init.d/apache2
restart' to activate new
configuration!

ramiro@ubuntu:~$
```

Aunque en la configuración se nos solicita reiniciar el servidor Web, aún no lo haremos.



Fichero de autenticación de usuarios.



Repositorio recién creado.

Creando el repositorio

Ahora debemos crear un nuevo repositorio de Subversion en el sistema, para que el servidor Apache pueda acceder a él y comunicarse.

```
ramiro@ubuntu:~$ sudo svnadmin
create /svn
ramiro@ubuntu:~$
```

A continuación, vamos a cambiar el propietario y los permisos del directorio "/svn", para que el servidor Apache pueda gestionar el repositorio correctamente.

Dado que el servidor se ejecuta bajo el usuario "www-data", haremos que éste pase a ser el nuevo propietario de los ficheros.

```
ramiro@ubuntu:~$ sudo chown -R
www-data.www-data /svn
ramiro@ubuntu:~$ sudo chmod -R
770 /svn
ramiro@ubuntu:~$
```

Llegados a este punto, debemos editar el fichero de configuración "/etc/apache2/mods-enabled/dav_svn.conf" y modificar los siguientes elementos:

- Descomentar las líneas "#<Location /svn>" (línea 13) y "#</Location>" (línea 54).
- Descomentar la línea "#DAV svn" (línea 16).
- Descomentar la línea "#SVNPath /var/lib/svn" (línea 19) y configurarla para que contenga la ruta al repositorio que creamos anteriormente, en nuestro caso "SVNPath /svn".
- Descomentar las líneas 40, 41 y 42, que contienen los parámetros "AuthType", "AuthName" y "AuthUserFile".
- Añadir, tras las líneas anteriores, una que rece "Require valid-user".

Ahora vamos a añadir un usuario al sistema de autenticación.

```
ramiro@ubuntu:~$ sudo htpasswd
-cm /etc/apache2/dav_svn.passwd
ramiro
New password:
Re-type new password:
Adding password for user ramiro
ramiro@ubuntu:~$
```

Para añadir un segundo usuario, debemos eliminar el modificador "-c" de la orden "htpasswd", pues el fichero ya se encuentra creado, y únicamente deseamos modificarlo.

```
ramiro@ubuntu:~$ sudo htpasswd
-m /etc/apache2/dav_svn.passwd
programador
New password:
Re-type new password:
Adding password for user
programador
ramiro@ubuntu:~$
```

Podemos comprobar que los usuarios han sido introducidos correctamente en el fichero.

```
ramiro@ubuntu:~$ cat /etc/
apache2/dav_svn.passwd
ramiro:$apr1$0QIDZ1aP$/
flnvsj1Y5acDWO4lH/HE0
programador:$apr1$WCf8SvX2$CXPyY
zODvSG0c9r9rH/yE.
ramiro@ubuntu:~$
```

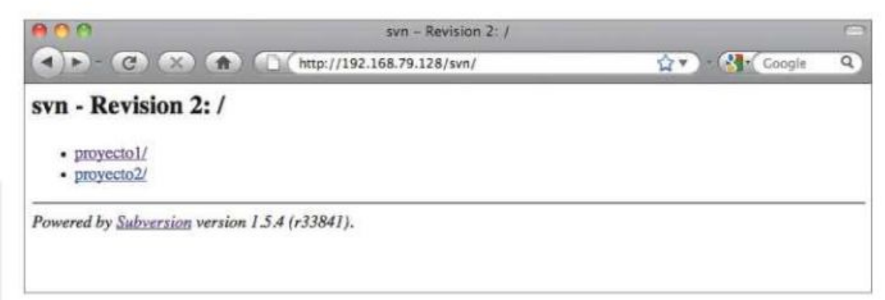
Ahora sí, es el momento de reiniciar el servidor Apache.

```
ramiro@ubuntu:~$ sudo /etc/init.
d/apache2 restart
 * Restarting web server apache2
        apache2: Could not
reliably determine the server's
fully qualified domain name, using
127.0.1.1 for ServerName
apache2: Could not reliably
determine the server's fully
qualified domain name, using
127.0.1.1 for ServerName
[ OK ]
ramiro@ubuntu:~$
```

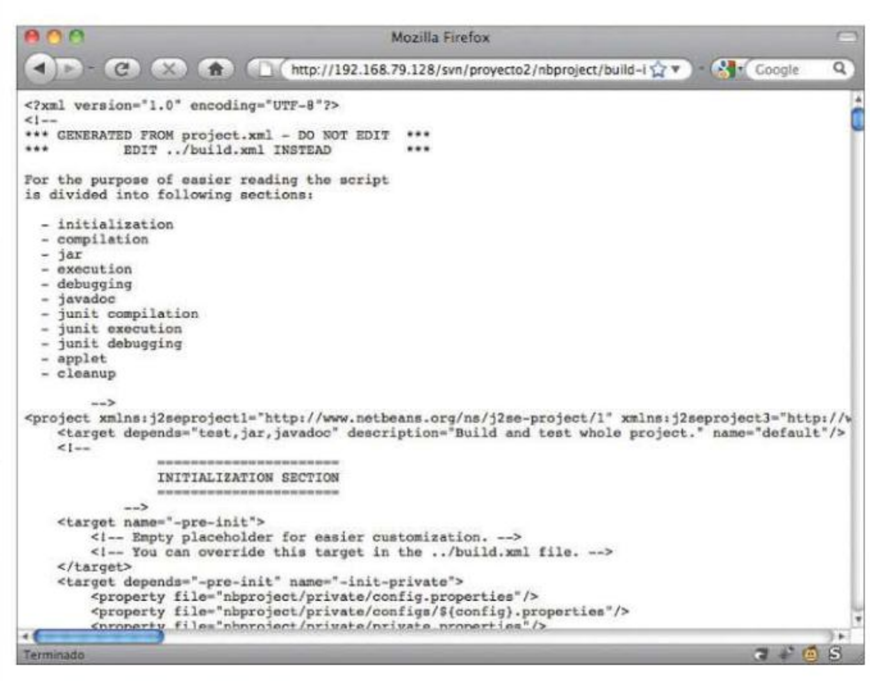
Accediendo al repositorio

Nuestro repositorio ya está configurado y listo para ser accedido. Si introducimos en la barra de direcciones de nuestro navegador la dirección "http://dirección/svn", podremos ver el mensaje de solicitud de credenciales que reza lo siguiente:

```
http://dirección está solicitando
un nombre de usuario y una
contraseña. El sitio dice:
"Subversion Repository"
```



Página del proyecto Subversión.



Metadatos de un proyecto NetBeans.

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */

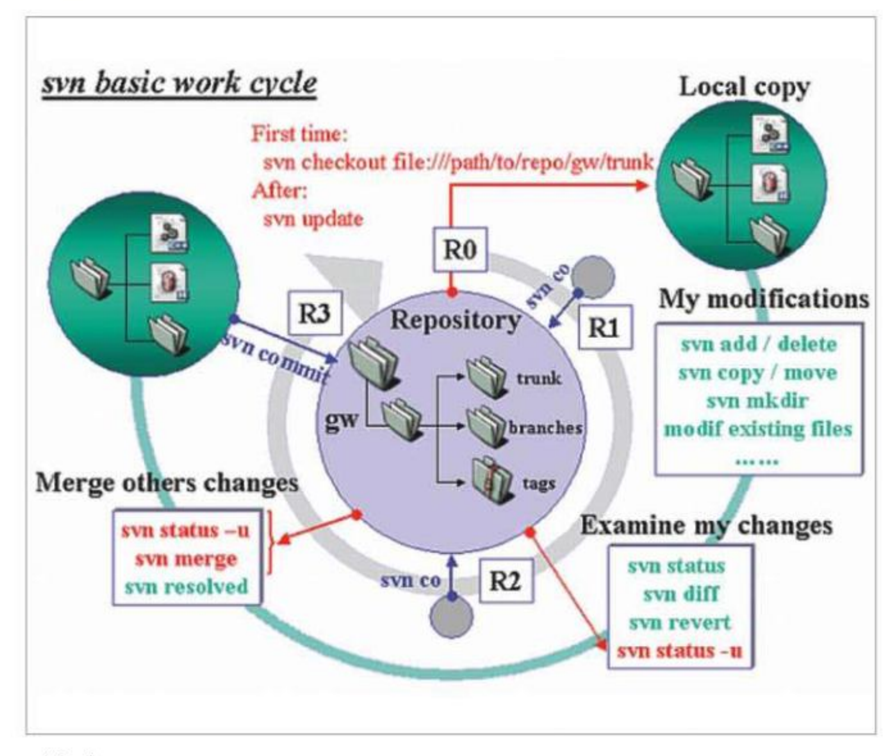
package proyecto1;

/**
 *
 * @author ramiro
 */
public class Main {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        // TODO code application logic here
    }

}
```

Código en el repositorio Subversión.



Ciclo de SVN.

Por defecto, el sistema no solicita contraseña para acceder al repositorio, si bien debido al hecho de haber incluido en la configuración la línea "Require valid-user", en nuestro caso sí que lo hará. Tras introducir el nombre de usuario y contraseña en el diálogo, accederemos al repositorio, que se encuentra de momento vacío.

```
svn - Revision 0: /
-
Powered by Subversion version
1.5.4 (r33841).
```

Para comprobar si el sistema funciona correctamente, vamos a configurar el servidor SVN en algún entorno de desarrollo de código y a subir un proyecto. Para este ejemplo, yo utilizaré el entorno de desarrollo para Java NetBeans.

Tras configurar los parámetros de acceso en el entorno, en el submenú de "Subversion" dentro del menú "Versioning", pulsaremos con el botón derecho sobre el proyecto y seleccionaremos la opción "Commit". Esta acción subirá los cambios existentes al repositorio, como podemos comprobar al acceder nuevamente al sistema a través del navegador:

```
svn - Revision 2: /

 * proyecto1/
 * proyecto2/
-
Powered by Subversion version
1.5.4 (r33841).
```

Si navegamos a la dirección "http://dirección/svn/proyecto1/src/proyecto1/Main.java", encontraremos el propio código fuente que hemos generador con el entorno de desarrollo.

```
/*
 * To change this template,
choose Tools | Templates
 * and open the template in the
editor.
 */

package proyecto1;

/**
 *
 * @author ramiro
 */
public class Main {

 /**
 * @param args the command line
arguments
 */
 public static void main(String[]
args) {
        // TODO code application
logic here
       }

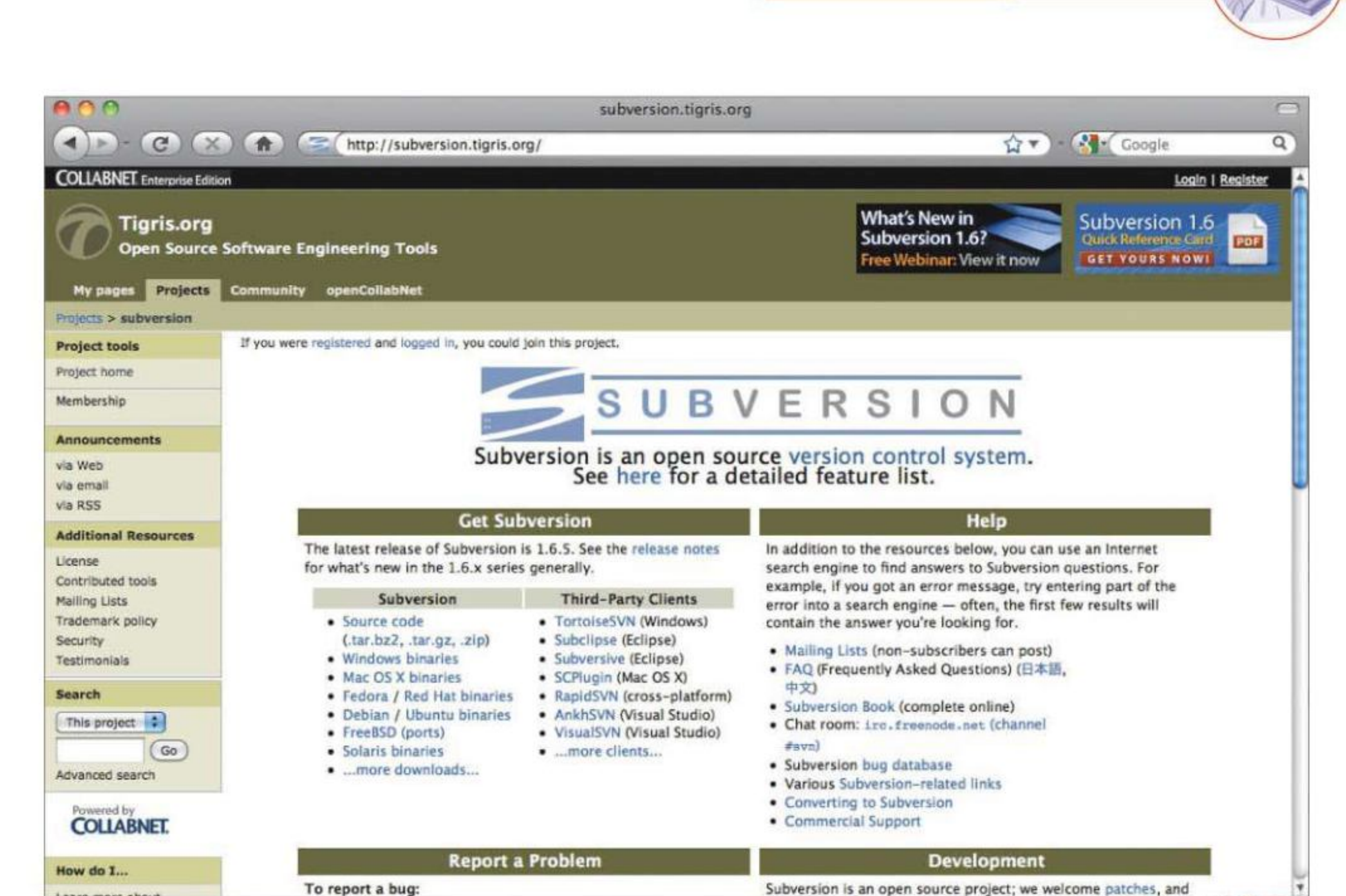
}
```

Por supuesto, podemos utilizar este repositorio con cualquier tipo de software compatible, y no únicamente con entornos de desarrollo de código. De hecho, es posible utilizar SVN directamente a través de la línea de comandos, pudiendo realizar cualquier operación implementada por el sistema.

```
ramiro@ubuntu:~$ svn --help
uso: svn <subcomando> [opciones]
[pars]
Cliente Subversion de línea de
comandos, versión 1.5.4.
Tipee 'svn help <subcomando>'
para ayuda sobre un subcomando
específico.
Tipee 'svn --version' para ver la
versión y los módulos de RA.
```



Solicitud de credenciales.



Página del proyecto Subversion.

```
o 'svn --version --quiet' para
ver sólo el número de versión.
```

La mayoría de los subcomandos reciben parámetros de tipo archivo y/o directorio. Si no se proveen parámetros a estos comandos, por omisión descenderán recursivamente desde el directorio actual (incluyéndolo).

```
Subcomandos disponibles:
 add
 blame (praise, annotate, ann)
 cat
 changelist (cl)
 checkout (co)
 cleanup
 commit (ci)
 copy (cp)
 delete (del, remove, rm)
 diff (di)
 export
 help (?, h)
 import
 info
 list (ls)
 lock
 log
 merge
 mergeinfo
 mkdir
 move (mv, rename, ren)
 propdel (pdel, pd)
 propedit (pedit, pe)
 propget (pget, pg)
 proplist (plist, pl)
 propset (pset, ps)
 resolve
 resolved
 revert
 status (stat, st)
 switch (sw)
 unlock
 update (up)

Subversion es una herramienta
para control de versiones.
Para información adicional, vea
http://subversion.tigris.org/
ramiro@ubuntu:~$
```

Terminando

Como habéis podido comprobar, desplegar un servidor SVN bajo un entorno GNU/Linux es un proceso muy sencillo. Además, y gracias a su capacidad para trabajar a través del protocolo HTTP, mediante el uso de DAV, es posible acceder a las funcionalidades de SVN mediante un simple servidor Web como Apache.

Además, y como ventaja añadida, permite la navegación por el contenido del repositorio utilizando únicamente un navegador Web.

Aún cuando no trabajéis con otras personas en el desarrollo de código, instalar un sistema de control de versiones resulta algo muy recomendable por orden, comodidad, y seguridad. Ya sabéis cómo hacerlo utilizando exclusivamente software libre en el proceso, por lo que ya no tenéis excusa. A programar se ha dicho.

¡Hasta la próxima!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/

Desarrollo de gadgets para Windows Vista

O cómo desarrollar un gadget y no morir en el intento.



Un Gadget no es ni más ni menos una aplicación que muestra la información que queramos de la forma que queramos o simplemente "que haga algo", lo que no tiene por qué tener el atributo "útil", aunque es recomendable si queremos que se utilice. Es decir, hace lo que nosotros queramos, dentro del marco de ejecución de Windows Vista y de las facilidades e limitaciones que este nos ofrece.

Estas herramientas nos permiten obtener información de una variedad de fuentes, presentarla de forma espectacular y además, siendo de gran utilidad. Son el complemento ideal del escritorio y, porque no, también complementan a las aplicaciones de escritorio usuale, Flickr3DCube s dado que nos permiten tener a la vista la información que deseemos, sean noticias, el tiempo, el estado de nuestros servidores, los hilos rss a los que estemos suscritos, notificaciones del mail, etc...



En este artículo se exponen las técnicas de desarrollo de sidebar gadgets para Windows Vista de un modo práctico ahondando en todas las facetas del desarrollo de un gadget "base" y en el "cómo desarrollar el gadget Flickr3DCube", gadget realizado con WPF y con la librería de 3D "3DTools" para WPF, desarrollada por Daniel Lehenbauer. Este gadget quedo en 2º lugar en el concurso de gadgets para Windows Vista "gadgetizate", organizado por el grupo de usuarios de Madrid, España y también ha aparecido mencionado en varios artículos como uno de los 15 gadgets más útiles e interesantes.



Control de versiones Sidebar Gadgets para Vista

Como muchos de vosotros ya sabréis, Windows Vista incorpora una barra lateral, sidebar, que alberga mini aplicaciones conocidas como "gadgets". Estos, de forma similar a los widgets de Mac OS o Linux, son unos diminutos pero no menos potentes programas que a modo de imanes de nevera se adhieren a nuestro escritorio y nos ofrecen variadas funcionalidades, algunas útiles y otras más divertidas, desde previsiones meteorológicas hasta monitorizar y controlar diferentes partes de nuestro equipo e incluso, de otros equipos.

Destaco la capacidad que nos ofrecen los gadgets para realizar y desarrollar todo aquello que podamos imaginar, de manera que esto nos aporte soluciones a necesidades que podamos tener, sean cuales sean. Los gadgets están basados en html y javascript como tecnologías principales para su desarrollo, siendo estos estándar conocido por muchos.

Lo bueno que tienen es que en su gran mayoría son gratuitos, por lo que son el complemento perfecto para que los programas tengan su presencia "útil" en el escritorio, como es el caso del Gadget de Nero, que nos permite iniciar el proceso de grabación de un cd o dvd desde el mismo escritorio, mostrándonos el proceso de la grabación de forma muy visual.

No obstante, y es una opinión, los gadgets vienen más de la mano de los servicios web - ofrecidos por "cloud", la nube - en cuanto a tener información "a la vista" en el escritorio permanentemente actualizada, como la evolución de valores bursátiles o el estado de diferentes equipos o servidores web de nuestra red o bien todo aquello que requiera transmitirnos información en tiempo real y de forma directa. Para este tipo de aplicaciones los gadgets son una solución ideal.

También lo son para todo aquello que requiera un pequeño espacio en nuestro escritorio y nos aporte "algo", como pueda ser un Chat, un programa de mensajería, un cliente de noticias vía rss, un cliente de galerías de imágenes online, etc..

Componentes de un gadget

Habiendo dejado bien claro que es lo que puede hacer un gadget es importante detallar la composición de los mismos. Antes de detallar las partes que componen un gadget es importante recalcar que en Windows Vista estos se basan exclusivamente en html, javascript y el modelo de objetos System.Gadget. Los Sidebar Gadgets son exclusivos de Windows Vista, cuya instalación ya aporta unos gadgets, pudiendo descargarnos más desde la Windows Live Gallery (**http://gallery.live.com/**). Estos gadgets, pese a ser en sí nada más que páginas web, se ejecutan en la máquina local, teniendo ciertos privilegios como el acceso a System.Gadget y a ciertos recursos locales.

El componente más importante del gadget es el gadget en sí mismo, esto es, un archivo que finaliza con la extensión ".gadget",

por ejemplo, "flickr3DCube.gadget". Un gadget no es más que un archivo comprimido con el estándar Zip (también podría venir como .Cab, pero no es corriente). En cualquier caso, si tenemos un gadget, tenemos sus fuentes html y javascript. De esta manera, se puede estudiar como están realizados para aprender y construir nuestro gadget perfecto o bien mejorar los que tengamos.Los gadgets tienen lo siguientes componentes:

- Archivo de manifiesto del gadget: Este archivo, de nombre gadget.xml, contiene la información necesaria para la instalación, ejecución y visualización de información del gadget en cuestión.
- Un archivo html para el "core" del gadget. Esto es, el gadget tal cual lo vemos en la sidebar.
- Un archivo html para la configuración. Es decir, que nos muestre la configuración actual y nos permita variarla. Esta es opcional, dado que puede que el gadget no necesite configurarse.
- Un archivo html para el "flyout". Esto es una ventana o panel que puede abrir y gestionar el gadget para mostrar información ampliada, como una fotografía más grande, ya que en el caso de haber hecho clic en una miniatura de una imagen, la intención más lógica sería visualizar la misma de forma ampliada.
- Imágenes, archivos de script y hojas de estilo. No cabe ni que decir que estos también son opcionales, pero nos harán mucho servicio bien utilizados por las páginas html que conforman el gadget.
- Iconos del gadget, para visualizar el gadget y su autor en el panel selector de gadgets, asimismo, también podemos determinar el icono que represente al gadget cuando lo arrastremos del panel a la SideBar.

Creando un gadget

Todo esto puede abrumar a más de uno, pero para que veáis que esto no son más que tecnicismos, vamos a desarrollar un gadget sencillo, un "hello Gadgeto-World!!" con un manifiesto y un archivo html bien sencillo. (luego, empezaremos con el cubo...:).

Ah, el entorno de desarrollo del gadget es Windows XP que es el entorno del que por ahora disponemos el 80% de los usuarios de Windows y también sobre el que he desarrollado el gadget en cuestión, utilizando otro equipo con Vista sólo para efectuar las pruebas.

Para empezar, crearemos un directorio que contendrá los diferentes elementos del gadget. Denominaremos a este directorio "hellogadget" y dentro de el crearemos el archivo de manifiesto, gadget.xml. Este tendrá la siguiente estructura:

```
<?xml version="1.0"
encoding="utf-8" ?>
<gadget>
  <name>HelloGadget!</name>
  <namespace>MsCoder.Gadgets</
namespace>
  <version>1.0.0.0</version>
  <author name="José Luis
Latorre">
        <info url="http://www.
brainsiders.com" />
  </author>
  <copyright>&#169; 2007</
copyright>
  <description>Otro Hola Mundo</
description>
  <hosts>
        <host name="sidebar">
        <base type="HTML"
apiVersion="1.0.0"
src="hellogadget.htm" />
        <permissions>Full</
permissions>
      <platform
minPlatformVersion="1.0" />
        </host>
  </hosts>
</gadget>
```

Leyendo el código xml básicamente se sobreentienden los diferentes componentes de este archivo, cuya estructura y secciones pueden ser ampliados con mayores prestaciones para ofrecer más características a nivel de gadget como por ejemplo una mayor información de este y de su autor. Por ahora, cabe destacar las siguientes secciones:

- La sección <name> define el nombre del gadget, este es el nombre que utilizará el panel de control de gadgets para identificarlo.
- La sección <author> contendrá información acerca del creador del mismo, aquí podéis indicar vuestro nombre, un enlace a vuestro blog o página web y también una imagen o logotipo que os identifique.
- La sección <host> es obligatoria y proporciona información acerca del "host" del gadget. Esto es, quien lo contiene y gestiona. En nuestro caso la única opción válida es "sidebar".
- La sección <base> especifica el tipo de gadget, actualmente sólo se permiten los gadgets del tipo "html". Se dejó a medias el tipo "wpf" lanzando los gadgets sólo con el desarrollo apto para este entorno (html + javascript). Supongo que en un futuro podremos hacerlo de forma nativa con herramientas 100% .net. Como prueba de ello, en http://www.stoyanoff.info, tenemos una guía de nombre "A Guide to Developing Windows Presentation Foundation Gadgets for Windows Sidebar" que nos muestra como hacer gadgets utilizando únicamente WPF (Windows Presentation Foundation).
- Por último, el atributo "src" de base nos indica el archivo que la SideBar debe de cargar para iniciar el gadget, en nuestro caso, la página web hellogadget.htm.

Para más información acerca del manifiesto del gadget, el referente es la documentación de MSDN (http://msdn2.microsoft.com/en-us/library/aa965879.aspx).

OJO, es importante recalcar que debemos grabar el archivo de manifiesto gadget.xml con la codificación UTF-8. Esto es importante o puede dar pie a errores. Seguido y no menos importante, crearemos la página principal del gadget, a la que previamente hemos denominado "hellogadget.htm". El archivo es el que sigue:

```
<html xmlns="http://www.
w3.org/1999/xhtml" >
<head>
  <title>HelloGadget!</title>
  <style>
  body {
        width:130;
        height:50;
  }
  </style>
</head>
<body>
        <span style="font-family:
Tahoma; font-size: 12pt;">¡¡Hola
```

```
Gadget!!</span>
</body>
</html>
```

Básicamente es una sencilla página Web a la que cabe destacar añadimos unos atributos vía estilos "inline" dentro del código html, para facilitar la comprensión y lectura, además que el tamaño de tales estilos y su uso en un único archivo html lo justifican.

Entre estos estilos tenemos los atributos que asignamos al cuerpo de la página "body" que son el ancho y alto del gadget en cuestión. Hemos de tener en cuenta que el ancho no debe superar el de la SideBar (o barra lateral) que está sobre unos 135/140 píxeles. De todos modos 130 píxeles es el tamaño máximo recomendado.

Instalación del Gadget
Instalando el gadget

Para instalar el archivo en Windows Vista debemos "empaquetar" el gadget como tal. Para hacer esto seleccionamos, dentro del directorio en el que hemos creado el gadget a todos los archivos y directorios, en nuestro caso, sólo tenemos dos:

- Gadget.xml
- Hellogadget.htm

Y los comprimimos en un archivo zip. Posteriormente editamos el nombre del archivo y cambiamos su extensión a .gadget, quedando su nombre cómo "hellogadget.gadget". Una vez hecho esto y habiendo copiado el gadget a un sistema con Windows Vista, tenemos dos formas de instalar el gadget. La primera y la más fácil radica en la instalación directa, para ello tenemos tres opciones:

- Mediante un doble clic en el gadget.
- Haciendo clic con el botón derecho del ratón sobre el gadget y seleccionar la opción "Add" o "Añadir".
- Arrastrando el gadget hacia la sidebar.
- La segunda, es la de los desarrolladores o "hackers", que implica el ubicar manualmente el gadget en el directorio de instalación.

Invocando la opción de ejecutar desde el menú de inicio (o vía la combinación "tecla Windows" + R) tecleando "%userprofile%\AppData\Local\Microsoft\Windows Sidebar\Gadgets" y pulsando en Aceptar se nos abrirá la carpeta física en la que nuestro usuario ubica sus gadgets. Esta será algo similar a "c:\users\nombre del usuario\appdata\local\Microsoft\windows sidebar\gadgets".

Allí copiaremos nuestro gadget. Este proceso es el mismo que el que realizan los demás.

También podríamos realizar los cambios directamente sobre estos archivos para probar de forma rápidamente ajustes y modificaciones.

En cualquier caso, tenemos nuestro primer gadget operativo, un gadget simple, pero ya hemos aprendido a desarrollar gadgets con su archivo de manifiesto, su página principal y a asignarle estilos. También hemos visto como instalarlos.

Concepto del gadget
Flickr3DCube, idea y evolución



El gadget de ejemplo, Flickr3DCube nació de un cubo, como indica su nombre, que vio la luz el 23 de Enero en una presentación de WPF, en la que participé como ponente, del grupo de desarrolladores .Net de Barcelona (http://www.bcndev.net) en ella se introdujo la teoría de WPF y luego una serie de exposiciones teórico-prácticas y acabamos montando un cubo en 3 dimensiones en el que cargábamos imágenes, archivos de video y los reproducíamos en cada una de las caras del cubo. Por último se realizó una versión "light" del cubo que manejamos con un mando de la consola Wii, de Nintendo, para demostrar las posibilidades de las 3D con otros controles más avanzados que un (ahora simple) ratón.

En los días siguientes, otro de los ponentes, nos "picó" sanamente a evolucionar el cubo, a añadirle interactividad, enlazarlo con webservices, que mostrase una galería de imágenes, que cargase video de youtube.com (o soapbox :P) así como irle otorgando mayores funcionalidades... aquí fue cuando nació la idea, después de realizar algunos ejercicios de interactividad entre el cubo, el escenario y el ratón, todo coincidió con el anuncio del concurso de gadgets a nivel nacional para Windows Vista organizado por el grupo de usuarios de .net de Madrid.

Y sí, estaréis pensando que si los gadgets no soportan otra cosa que html que el cubo en cuestión es WPF, pues bueno, lo transformamos en XBAP (Xml Browser APplication) y listo!! Ya podemos incluirlo dentro de un iframe en un archivo xml...
De hecho hay varias formas de realizarlo pero a cada cual más compleja... la más sencilla que conseguí que funcionase fue esta, la conversión del wpf a xbap y su inclusión vía iframe en el gadget. Tuvo su precio, no obstante, que ya comentaré más adelante.

Seguido veremos el manifiesto y la página principal del Flickr3DCube, algo más ampliados que en el ejemplo de "HelloGadget!" inicial.

Manifiesto:

```
<?xml version="1.0"
encoding="utf-8" ?>
<gadget>
  <name>Flickr3DCube Gadget</
name>
  <namespace>Flickr3DCube</
namespace>
  <version>1.0.0.0</version>
  <author name="José Luis
Latorre">
        <info url="http://bcngeek.
com/"/>
        <logo src="developer.
png"/>
  </author>
  <copyright>&#169; 2007</
copyright>
```

```
  <description>Gadget
Visualizador de imagenes Flickr
en 3D</description>
  <icons>
        <icon height=”96”
width=”84” src=”flickr3dcube.
png”/>
  </icons>
  <hosts>
  <host name=”sidebar”>
        <base type=”HTML”
apiVersion=”1.0.0” src=”default.
html”/>
        <permissions>full</
permissions>
        <platform
minPlatformVersion=”1.0”/>
        </host>
  </hosts>
</gadget>
```

Como detalle, añadimos un logo o imagen del desarrollador, en la sección <copyright> hemos puesto el carácter © mediante el código html © Y hemos añadido un icono con la sección <icons>. Este será el icono que aparecerá en la galería de gadgets de Windows Vista.

Como Flickr3DCube no dispone de página de configuración ni del flyout, estos se omiten en este archivo de manifiesto de gadget.

Luego, tenemos el fuente del archivo fuente default.html, cabe decir que pese al nombre asignado podríamos poner cualquier otro cómo Flickr3DCube_Main.html, por ejemplo. El código del mismo es este:

```
<html>
<head>
<title>Flickr3DCube</title>
<style>
  body {
        width:140;
        height:160;
        padding:5;
        margin:0;
        background:DimGray;
  }
</style>

<script type=”text/javascript”>
function loadMain()
{
  System.Gadget.onDock = dock;
  System.Gadget.onUndock =
unDock;
  dock();
}

function unDock()
{
  document.body.style.width =
300;
  document.body.style.height =
300;
  document.getElementById('Flickr
3DCubeFrame').width=
        290;
  document.getElementById('Flickr
3DCubeFrame').height=
        290;
}

function dock()
{
  document.body.style.width=140;
  document.body.style.height=160;
  document.getElementById('Flickr
3DCubeFrame').width=
        130;
  document.getElementById('Flickr
3DCubeFrame').height=
        150;
}
</script>
</head>

<body onload=”loadMain()”>
  <iframe id=”Flickr3DCubeFrame”
        height=”150”
        width=”130”
        src=”Flickr3DCube.xbap”/>

</body>
</html>
```

El código es sencillo y al ser un único archivo de código fuente no he puesto los estilos en un archivo css externo; y lo mismo he hecho con las rutinas javascript ya que son muy breves y de esta forma queda todo el código a la vista y muy claro.
La página está compuesta de un único componente, un iframe de nombre Flickr3DCubeFrame al cual le asignamos unas dimensiones de 130 píxeles de ancho y 150 de alto ya que, dado que contendrán un espacio de trabajo y el cubo es menor que el mismo para permitir una cierta interactividad, debía hacerlo cuanto más grande mejor. Luego asignamos como contenido de dicho gadget (src) a la aplicación XBAP (Xaml Browser APplication), de nombre Flickr3DCube.xbap.

El resto del código gestiona el amarre y desamarre del gadget (Docking y unDocking). Es decir, cuando lo “amarramos” a la SideBar “barra lateral”, realizando el Docking, se posiciona y queda estático en la barra lateral de gadgets, o bien si lo “desamarramos”, realizando el unDocking, queda libre, no quedando limitado al tamaño de la SideBar , de manera que se pueda ubicar en cualquier parte del escritorio.

Si os fijáis en los estilos, el body está a 140 píxeles pero el iframe a 130; esto es para dejar un marco entre medio que nos servirá para “agarrar” el gadget y desplazarlo para cambiarlo de ubicación en la toolbar o para desacoplarlo de la misma (undock) y dejarlo en el escritorio. Como el tamaño inicial está limitado por el ancho de la Sidebar, cuando lo dejamos en el escritorio nos interesa ampliar el espacio de trabajo del gadget, cosa que hacemos mediante los eventos Gadget.onUndock y Gadget.onDock. En el código fuente tenemos la función loadMain:

```
function loadMain()
{
  System.Gadget.onDock = dock;
  System.Gadget.onUndock =
unDock;
  dock();
}
```

que asocia la función dock como handler del evento onDock y la función unDock como handler del evento onUndock. Seguido llamamos a dock, puesto que los gadgets se inicializan por defecto en la SideBar. La función dock es sencilla:

```
function dock()
{
  document.body.style.width=140;
  document.body.style.height=160;
  document.getElementById('Flickr
3DCubeFrame').width=130;
  document.getElementById('Flickr
3DCubeFrame').height=150;
}
```

Ponemos el tamaño de la página a 140 píxeles de ancho por 160 de alto y ajusta-

mos el tamaño del iframe en consonancia, a 130 píxeles de ancho por 150 de alto. El espacio sobrante es para permitir un espacio que controle el html mediante el cual poder realizar drag & drop con el gadget. En cuanto a la función undock, otro tanto de lo mismo:

```
function unDock()
{
  document.body.style.width =
300;
  document.body.style.height =
300;
  document.getElementById('Flickr
3DCubeFrame').width=290;
  document.getElementById('Flickr
3DCubeFrame').height=290;
}
```

Al contrario que dock, undock establece el tamaño de la página a 300 píxeles, tanto de ancho como de alto y el tamaño del iframe a diez píxeles menos, 290, con lo que ya queda un espacio de trabajo decente para que el gadget se luzca.

Cabe destacar que de tener más páginas (flyout, configuración, etc..) se hubieran separado los archivos de estilo y los de script en sendos Flickr3DCube.css y Flickr3DCube.js, por ejemplo, en aras de no repetir el estilo y el código en cada una de las páginas... y mantenerlo doblemente en caso de ser necesarias modificaciones.

Para no omitir la estructura de dichas páginas, dado que este es un artículo sobre gadgets, no vamos a obviarlas, sino que las veremos en unos sencillos ejemplos todo seguido.

Configurando el gadget

Los gadgets tienen la habilidad de mostrar un diálogo de configuración al usuario y también pueden almacenar y recuperar dichas configuraciones mediante la propia API de los gadgets. De hecho la configuración la mantiene sin problemas para múltiples instancias de gadgets sin realizar ningún tipo de desarrollo adicional.

Esta configuración la realizaremos, cómo no, desde una página html que será la que se visualizará cuando el usuario pulse el icono de configuración del gadget. La página en cuestión sería "configuracion.html", cuyo código exponemos a continuación:

```
<html xmlns="http://www.
w3.org/1999/xhtml">
<head>
  <script type="text/javascript"
src="configuracion.js"></script>
       <link href="configuracion.
css" rel="stylesheet" type="text/
css" />
</head>
<body>
       Saludamos a:
       <br />
       <input name="SaludoA"
type="text" maxlength="50" />
</body>
</html>
```

En esta página básicamente tenemos un cuadro de texto en el que se puede poner el nombre de la persona que saludaremos con el "hola gadget" que hemos implementado en nuestro primer ejemplo. El propio entorno del gadget nos proporcionará un botón de "OK" y de "Cancel" para la interacción con el usuario; nosotros sólo necesitaremos realizar la carga y la grabación de este nombre en la configuración del gadget.

La página referencia a un archivo de estilos css que es "configuracion.css":

```
body
{
  width:200;
  height:85;
}
```

Y por último ubicamos toda la lógica en el archivo de script "configuracion.js":

```
document.onreadystatechange =
function()
{
  if(document.
readyState=="complete")
  {
  var sSaludoA = System.Gadget.
Settings.read("SaludoA");
       if(sSaludoA!= "")
       {
       SaludoA.value = sSaludoA;
  }
  }
}

System.Gadget.onSettingsClosing =
function(event)
{
  if (event.closeAction == event.
Action.commit)
  {
       var sSaludoA = SaludoA.
value;
       if(sSaludoA!= "")
       {
       System.Gadget.Settings.
write("SaludoA ", SaludoA);
       }
       event.cancel = false;
  }
}
```

Básicamente, asignamos la primera función al evento de cambio del estado de la página "onreadystatechange" y cuando el estado es "complete" es decir, que ha cargado la página de configuración, recupera el valor de la variable de configuración "SaludoA" y si no está vacía la asigna al cuadro de texto.

Esto podríamos asociarlo también al evento onload de la página, pero este método es más óptimo y evita posibles errores. No obstante el código quedaría así:

```
<body onload="CargarConfiguracio
n()">
```

La segunda función se invoca cuando cerramos el diálogo de configuración del gadget, enlazando System.Gadget.onSettingsClosing al código que definimos. Podríamos declarar la función de forma separada, como hemos hecho previamente con dock e undock, (que es básicamente lo mismo), sólo que aquí evitamos que cualquier otro evento llame a la función ya que queda asignada de forma inequívocamente al handler de este evento. En cualquier caso, esta función valida que la acción de cierre sea el botón de "OK" para proceder a grabar la configuración, cosa que hace dentro del namespace propio de la configuración de gadgets "System.Gadgets.Settings", con el método write. Luego deberíamos adaptar el primer código fuente para que muestre el contenido de la variable de configuración.

```
<html xmlns="http://www.w3.org/1999/
xhtml" >
```

```
<head>
  <title>HelloGadget!</title>
  <style>
  body {
        width:130;
        height:50;
  }
        #HolaGadget
        {
        width: 130px;
        top: 25px;
        text-align: center;
        font-family: Tahoma;
        font-size: 12pt;
        position: absolute;
        }
  </style>
  <script>
        var sSaludoAPorDefecto =
"¡¡Hola Gadget!!";
        System.Gadget.settingsUI
= "configuracion.html";
        System.Gadget.
onSettingsClosed =
CargarConfiguracion;

        function EstablecerTexto()
  {
        var sSaludoA = System.
Gadget.Settings.read("SaludoA")
        if(sSaludoA!= "")
        {
        HolaGadget.innerText =
sSaludoA;
        }
        else
        {
        HolaGadget.innerText =
sSaludoAPorDefecto;
        }
        }

        function CargarConfiguraci
on(event)
        {
        if (event.closeAction ==
event.Action.commit)
              {
        EstablecerTexto();
        }
  }

  </script>
</head>
<body onload="EstablecerTexto();">
<div id="HolaGadget"></div>
</body>
</html>
```

Básicamente en el script asocio la página de configuración a configuracion.html

```
System.Gadget.settingsUI =
"configuracion.html";
```

Esto hará que la marca de configuración del gadget se active, pudiendo hacer clic en ella para abrir la página de configuración que hemos asociado al gadget.

Seguido, asocio el evento de cierre de la página de configuración a la función CargarConfiguracion:

```
System.Gadget.onSettingsClosed =
CargarConfiguracion;
```

Esta, refrescará el contenido de la página principal del gadget si hemos cerrado la ventana de configuración haciendo clic en el botón de OK.

```
function CargarConfiguracion(eve
nt)
{
  if (event.closeAction == event.
Action.commit)
        {
        EstablecerTexto();
  }
}
```

Y en el evento "onload" de la página recuperamos la variable de configuración y, si está vacía ponemos un valor por defecto.

```
<body onload="EstablecerTexto()
;">
```

Esto lo hacemos con la función EstablecerTexto que recupera la configuración del gadget, cargando el valor en una variable:

```
var sSaludoA = System System.
Gadget.Settings.read("SaludoA")
```

Y, si el valor recuperado está vacío, asignamos un valor por defecto previamente definido.

```
if(sSaludoA!= "")
{
  HolaGadget.innerText =
sSaludoA;
}
else
{
  HolaGadget.innerText =
sSaludoAPorDefecto;
}
```

Con esto ya tendríamos implementada la configuración del gadget sobre el potente sistema que nos aporta el Windows Vista en el namespace de System.Gadget.Settings.

Y ahora, el Flyout

Lo único que nos quedaría por ver sería cómo implementar una ventana de "flyout" en un gadget. Un flyout es una ventana que puede abrir y gestionar el gadget para visualizar información adicional o bien visualizar la misma información que el gadget pero teniendo una mayor superficie de trabajo para hacerlo.

Su nombre viene de que esta se abre siempre de forma flotante (fly) y fuera de la SideBar (out).

Trabajar con un flyout en un gadget es tremendamente sencillo, para mostrar un flyout, por ejemplo con tan sólo el siguiente código:

```
System.Gadget.Flyout.file =
"Flyout.html";
System.Gadget.Flyout.show = true;
```

Asignamos la página Flyout.html como flyout del gadget y con la siguiente instrucción, la hacemos visible.

Para ocultarla, tenemos la instrucción inversa:

```
System.Gadget.Flyout.show = true;
```

Por ejemplo, para abrir el flyout al hacer clic en un enlace, escribiríamos:

```
<a href="" onclick="showFlyout();
">Ver Flyout</a>
```

Es decir, asignamos una función javascript que nos cargará el flyout del gadget.

Luego, escribiremos la función showFlyout() que añadiremos al script de la página html principal del gadget, "hellogadget.htm":

```
function showFlyout ()
{
        if ( System.Gadget.
Flyout.show == false )
  {
        System.Gadget.Flyout.file
= "Flyout.html";
        System.Gadget.Flyout.show
= true;
  }
  else
        hideFlyout() ;
}

function hideFlyout ()
{
 System.Gadget.Flyout.show =
false;
}
```

Al hacer clic llamamos a showflyout, que si el flyout está oculto, lo visualizará y si está visible, lo ocultará...

Y la parte menos importante, la página html Flyout.html podría ser algo similar a esto:

```
<html xmlns="http://www.
w3.org/1999/xhtml" >
<head>
  <title>HelloGadget! - Flyout -</
title>
  <style>
  body {
        width:260;
        height:90;
  }
  </style>
</head>
<body>
        <span style="font-family:
Tahoma; font-size: 18pt;">Flyout de
¡¡Hola Gadget!!</span>
</body>
</html>
```

Y sólo quedaría paquetizar el gadget e instalarlo de la forma previamente descrita. Con esto



Fig.1

tendríamos un gadget plenamente funcional y operativo, con todas las características propias de un gadget implementadas adecuadamente.

Una vez instalado, lo probaremos haciendo doble clic en la imagen del gadget mismo para crear una instancia en el escritorio (**fig.1**).

Y nos aparecerá el gadget en la SideBar:



Sí hacemos clic en el icono de configuración, representado por una llave inglesa, se nos abrirá la ventana de configuración:



Introducimos un texto y pulsamos el botón de Aceptar, "Ok" en inglés. Luego, si pulsamos el botón de "Ver Flyout", veremos la siguiente pantalla:



Para ocultar el flyout, pulsaremos el enlace "Ocultar Flyout". Y con esto finalizamos el recorrido por las funciones básicas del gadget que hemos desarrollado a lo largo de este artículo.







Hardware bajo llave

Los discos duros portátiles y las llaves de memoria USB también son vulnerables al malware. Para garantizar que la información viaje siempre a salvo, existen productos concretos como las copias de seguridad, el hardware encriptado o las contraseñas imposibles de averiguar.

Seguridad y más seguridad. Cualquier medida que se tome para frenar el avance y la propagación de los ataques de los hackers y los virus y códigos malignos en forma de phising o troyanos, entre otros, parece ser poca. En este contexto, hay que tener en cuenta que su divulgación no sólo tiene lugar a través de la Red, sino también mediante dispositivos de almacenamiento portátiles como las llaves de memoria USB y los discos duros externos, dos categorías de producto cuya popularidad ha crecido como la espuma en los últimos años. Y es que motivos no les faltan: sus capacidades de almacenamiento son cada vez mayores y sus precios más asequibles, características a las que se suma un sencillo y cómodo transporte.

Especialmente significativo es el último informe mensual del proveedor global de protección de antivirus ESET, que revela los datos referidos a la detección de amenazas informáticas en nuestro país el pasado mes de septiembre. En dicho informe se ha constatado que, en lo más alto de la tabla, siguen estando los mismos códigos maliciosos de meses anteriores (INF/Autorun con un 10,03% de las detecciones, Win32/Conficker con un 7,23% y Win32/PSW.OnLineGames con un 6,67%) y que hay que seguir concienciando a los usuarios sobre la importancia de adoptar medidas básicas desde el punto de vista de la seguridad. Así, ESET insiste en la necesidad de controlar el uso de los dispositivos de memoria extraíbles de los equipos ya que su auto ejecución es responsable de una parte importante de las amenazas más difundidas en España. Tal y como ha declarado Fernando de la Cuadra,

>>> BLINDA TU USB

En el supuesto de que tu llave de memoria no tenga ningún tipo de seguridad y no quieras comprarte otra porque prefieres aprovechar la que ya tienes, en la Red es posible encontrar programas gratuitos (y bastante sencillos de utilizar) que te permiten crear un fichero cifrado protegido. Una de estas herramientas es el software TrueCrypt que puedes descargarte desde la dirección: www.truecrypt.org. Cuando lo hayas hecho, y tras aceptar las condiciones de uso de la página y completar el proceso de instalación (no olvides reiniciar el sistema), te encontrarás con el icono que te permite iniciar TrueCrypt. Pínchalo y escoge el botón "Crear Volumen": su asistente de creación de volúmenes te muestra una ventana de trabajo con tres opciones. En este caso, hay que escoger la primera para crear el archivo cifrado. En la siguiente ventana, la casilla a activar es "Volumen TrueCrypt Común". Cuando se ha llegado a este punto, lo próximo es decidir la ubicación y el nombre que recibirá al archivo cifrado. También escogeremos el algoritmo de cifrado a emplear (por ejemplo, AES); el tamaño del archivo y su contraseña. Finalmente, sólo quedaría formatear el fichero en el sistema de archivo deseado. Para acceder, en cualquier instante, al contenido de la llave lo único que hay que hacer es abrir el programa y pulsar sobre opción "Montar". TrueCrypt lo montará en el sistema al introducir la contraseña que previamente le hayamos indicado y asignándole la letra de unidad elegida.

director de Educación de Ontinet.com, distribuidor de los productos de seguridad de ESET: "El intercambio de archivos entre distintos usuarios, y entre diferentes equipos a través de las conexiones USB, sigue siendo un vector de infección importante". Y añade: "Ello a pesar de las reiteradas alertas lanzadas por firmas de seguridad a los usuarios para que vigilen en todo momento dónde conectan sus dispositivos y qué tipo de información almacenan en los mismos".

Ante una situación de estas características, la pregunta que uno, casi de manera obligatoria, se plantea es la siguiente: ¿Qué puedo hacer como usuario de esta clase de soluciones de almacenamiento móvil? Además de seguir tomando conciencia sobre la importancia de proteger la información crítica, una alternativa a destacar es la utilización de dispositivos de memoria USB encriptados y basados en hardware. Se trata de una opción que proporciona niveles de protección significativos con la que mantener los datos a buen recaudo, aunque no la única. Otras posibilidades son los antivirus específicos para este tipo de productos como MX One (www.mxone.net) o la creación de varias particiones dentro de una misma unidad. Por ejemplo, una privada de carácter restringido y otra pública de libre acceso. Nosotros nos hemos querido centrar en el cifrado por hardware.

Hardware

Hace tiempo que la encriptación viene perfilándose como una de las tecnologías vitales capaces de asegurar que las tareas de almacenar, transmitir y compartir información ganen en seguridad para tranquilidad del usuario. La clave se encuentra en el empleo de un conjunto de herramientas que cifran los datos y que al resultar ilegibles son, por lo tanto, imposibles de interpretar a no ser que se sepa hacerlo correctamente. Este cifrado puede aplicarse a diversos archivos y ficheros: desde un documento de texto

>>> LLAVES USB CIFRADAS

EMTEC S450 AES FLASH DRIVE

Esta solución de almacenamiento móvil emplea hardware encriptado de 256 bits. Para activar tanto la encriptación como la desencriptación, incorpora un programa autenticador de contraseña. En el caso de producirse seis intentos fallidos de identificación, la llave se bloquea definitivamente y la información no se muestra accesible. Con una velocidad de lectura de 25 Mbytes/segundos y 15 Mbytes/segundos de escritura, su cubierta de goma la hace resistente. **Precio:** 4 Gb (34,90 euros), 8 Gb (44,90 euros), 16 Gb (69,90 euros), 32 Gb (129 euros). **www.entec-international.com**



KINGSTON USB DATATRAVELER LOCKER

Se trata de una llave USB encriptada basada en un sistema de encriptación AES de 256 bits en la que se distingue una zona pública y otra encriptada que garantiza la seguridad de los datos almacenados. Para ello, la unidad está preparada para bloquearse y, posteriormente, reformatearse tras 10 intentos de accesos que no estén autorizados. Tiene unas dimensiones de 65,76 mm x 17,98 mm x 10,7 mm. **Precio:** 4 Gb (18,56 euros), 8 Gb (34,05 euros) y 16 Gb (63,98 euros). **www.kingston.es**



SANDISK ULTRA BACKUP

Ha sido diseñada para proteger cualquier tipo de archivo digital, motivo por el cual la memoria los protege a través del sistema de doble capa con control de acceso a través de contraseña y cifrado AES. Todos estos procesos se efectúan de manera automática, sin que el usuario lo perciba en ningún instante. Su otra gran ventaja es que efectúa copias de seguridad de los datos que hay almacenados con sólo pulsar un único botón, y sin necesidad de tener que instalar ningún software adicional. **Precio:** 8 Gb (33,90 euros), 16 Gb (55,90 euros), 32 Gb (110,90 euros) y 64 Gb (222,90 euros). **www.sandisk.es**



IMATION PIVOT USB FLASH DRIVE

Presenta un diseño pivotante y una carcasa duradera y resistente al agua que está fabricada en caucho para encarar mucho mejor los desplazamientos. Está disponible en diferentes capacidades y soporta, al igual que otros productos que hemos recogido en este bazar, un sistema de encriptación AES de 256 bits. A nivel de seguridad, además, el modelo concede la posibilidad de almacenar la información en áreas públicas o privadas para garantizar un mejor control de los datos que el usuario maneja. Es compatible con Windows Vista ReadyBoost. **Precio:** 2 Gb (11,90 euros), 4 Gb (13,90 euros), 8 Gb (22,90 euros) y 16 Gb (45,90 euros). **www.imation.com**



en Word a una base de datos en Excel, pasando, incluso, por mensajes de correo electrónicos ya que existen herramientas que permiten que viajemos junto a nuestros e-mail y páginas de Internet preferidas.

La encriptación basada en hardware desde hace unos cuantos años viene ganando terreno a la basada en software porque esta última se muestra más lenta y vulnerable. Hay que pensar, a este respecto, que si nos sustraen nuestro dispositivo (o alguien hace una copia de él), y sólo lo protegemos de manera exclusiva con un programita que salvaguarde nuestros archivos más

>>> TUS DATOS CONTIGO Y SIEMPRE A SALVO

La protección por hardware es una de las posibilidades que ofrece el mercado para garantizar el mantenimiento seguro de los datos, pero existen otras soluciones más sencillas, que resultan igual de válidas: hay que tener en cuenta que no todas las llaves USB o los discos duros incorporan de serie la tecnología de cifrado de hardware que hemos explicado. Nosotros nos referimos a la posibilidad de proteger la lectura de la información mediante contraseña. El software que incorporan estos dispositivos permite, asimismo, llevar a cabo copias de seguridad y sincronizar contenidos con el ordenador. Un ejemplo lo tenemos en el programa JetFlash elite 2.0 de Transcend: destinado a incrementar la productividad de los usuarios, está pensado para utilizarse con sus llaves de memoria USB JetFlash. Este software comprime los archivos guardados mediante contraseña y brinda la posibilidad de actualizar la información que se maneja (función DataBackup) con un solo clic. También guarda una copia de los favoritos de Internet y el correo personal. Por otro lado, el programa para discos duros de Transcend StoreJet elite 3 propone prestaciones muy similares maximizando la capacidad de memoria disponible.

VERBATIM USB BUSINESS SECURE



Tiene un diseño que permite proteger sus conectores USB mediante un mecanismo retráctil, haciendo innecesario utilizar un capuchón protector. Está certificada para Windows Vista y la memoria que incorpora ofrece varias funciones desde el punto de vista de la seguridad: este es el caso del sistema de acceso mediante password. Protege a la llave del ataque de los hackers borrando los datos guardados tras seis intentos fallidos de introducir la contraseña correcta. Con un sistema de encriptación por hardware AES de 256 bits, existe la opción de adquirir por separado el programa Endpoint Protector. Su función es rastrear las trasferencias a través de dispositivos de almacenamiento portátiles que sólo utilicen los PCs registrados. **Precio:** 8 Gb (79 euros) y 16 Gb (99 euros). **www.verbatim.com**

preciados, corremos el riesgo de que éstos sean finalmente descubiertos: las técnicas de los usuarios malintencionados son cada vez más inteligentes y precisas. Otra característica significativa del cifrado por hardware es que no requiere de un gasto de procesamiento de la CPU del ordenador, una particularidad que permite que el rendimiento del sistema se optimice y vaya más rápido.

Ventajas principales

El hecho de que una solución de almacenamiento portátil incorpore hardware criptográfico implica aportar mayor seguridad y rapidez a la solución en cuestión. Las llaves flash USB y los discos duros criptográficos que se basan en un hardware que genera, almacena y protege las claves cifradas también se conocen con el término de Módulo de Seguridad por Hardware (HSM). Para que lo entendamos un poco mejor, las claves que utilizan quedan guardadas en una especie de módulos a modos de placas. Resultan especialmente seguros porque, en este caso, las claves del cifrado que se emplean no están junto a los datos del cifrado. Otro dato que hay que tener en cuenta es que las claves protegidas lo estarán siempre (y plenamente) cuando éstas hayan sido generadas en el propio hardware. De lo contrario, ese candado de seguridad corre el riesgo de que se fuerce y quede abierto. Existen fabricantes que también brindan hardware HSM que incorporan conectividad de red y que protegen los datos de todos aquellos sistemas que están conectados entre sí.

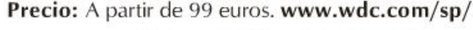
El estándar AES

Suele ser habitual que los sistemas de encriptación por hardware empleen el algoritmo Advanced Encryption Standard (AES), cuyos orígenes están ligados al gobierno de Estados Unidos ya que decidió adoptarlo como estándar de cifrado. Dicho esquema está organizado a modo de bloque y constituye, en la actualidad, uno de los sistemas de cifrado más empleados y que viene especificado por una clave máxima de 256 bits. Acceder a la información, en este caso, resulta imposible. También es común que, por ejemplo, si un usuario que no está autorizado a utilizar una llave de USB intenta acceder a su contenido, éste se borre completamente tras un número determinado de intentos fallidos.

>>> DISCOS DUROS BAJO LLAVE

WESTERN DIGITAL MY BOOK ESSENTIAL

Capacidad de almacenamiento, copia de seguridad visual y cifrado mediante hardware. Estas tres características definen la naturaleza del disco duro My Book Essential de Western Digital, una solución de almacenamiento con un formato similar al de un libro e interfaz USB 2.0. Disponible en distintas capacidades (500 Gb, 1 Terabyte, 1,5 Terabytes y 2 Terabytes), incorpora un indicador luminoso para saber cuánto espacio queda disponible en el disco. A nivel de seguridad ofrece protección mediante contraseña que se combina con un cifrado de 256 bits mediante hardware para codificar la información antes de almacenarse. El software WD SmartWare permite realizar copias de seguridad personalizables, un proceso que puede seguirse visualmente. Las copias de seguridad tienen un carácter automático y continuo cada vez que se añade o se modifica un fichero. **Precio:** A partir de 99 euros. **www.wdc.com/sp/**





IOMEGA EGO ENCRYPT 320 GB

Con unas dimensiones de 141,5 x 97,5 x 23,1 mm y un peso de 268 gramos, Iomega nos propone este disco duro portátil en color plata e interfaz USB 2.0 que no requiere una fuente de alimentación externa y que, además, no consume recursos de memoria. Su diseño resulta duradero, incorporando una banda de protección para mayor estabilidad gracias a su tecnología Drop Guard. La seguridad en este modelo corre a cargo de un sistema de cifrado por hardware y dos programas: el software EMC Retrospect HD, su descarga es gratuita y crea copias de seguridad fácilmente, y MozyHome para realizar backups en línea. **Precio:** 99,90 euros. **www.iomega.com**

LACIE D2 SAFE HARD DRIVE

Está construido sobre una robusta aleación de aluminio en la que se ha integrado una triple interfaz: USB 2.0 (un puerto), Firewire 800 (dos puertos) y Firewire 400 (un puerto). Codifica los documentos automáticamente mediante cifrado de hardware AES de 128 bits, una medida de seguridad que se suma a la huella dactilar. En este caso, el producto de LaCie está preparado para registrar un máximo de 10 huellas (5 usuarios con 2 huellas cada uno) que bloquearán o desbloquearán el disco con sólo colocar un dedo en la zona correspondiente. Es posible, asimismo, establecer privilegios de acceso (por ejemplo, sólo lectura o lectura y escritura). Para ganar espacio en el escritorio, el producto puede colocarse verticalmente. **Precio:** 399 euros (2 Terabytes). **www.lacie.es**





147

FRIKI GADGET

LO MAGICO DE UN DíA DE COMPRAS





Los entresijos del cibercrimen, una actividad muy lucrativa

Tarjetas de crédito, ataques informáticos, envíos spam o bases de datos repletas de datos personales o de direcciones de correo electrónico se venden en los bajos fondos de Internet. Incluso, a veces, estos productos se anuncian con banners publicitarios y se ofrecen descuentos por volumen, o devuelven el dinero si, por ejemplo, los datos de la tarjeta de crédito que han proporcionado no funcionan.

Los datos robados de una tarjeta de crédito tienen un precio de mercado de unos 300 < Un ataque DDoS (Distributed Denial of Service, ataque que satura e inutiliza los servidores de las víctimas) de una hora de duración puede costar unos 150< Y se pagan hasta 800 euros por un millón de correos spam. Estas y otras cifras se recogen en el libro blanco 2009 "La economía sumergida" elaborado por Marc-Aurél Ester y Ralf Benzmüller de G Data Security Labs y disponible en http://www.gdata.es. El equipo de G Data Software se camufló en los círculos de acción de hackers, ladrones de datos y demás delincuentes digitales durante los meses de junio y julio de este año y descubrieron que el escenario se ha profesionalizado al máximo dando lugar a una economía perfectamente organizada. Al frente de la organización existen proveedores que ofrecen 'hosting a prueba de balas' que permiten la existencia de foros y tiendas online ilegales en las que los ciberdelincuentes ofrecen sus servicios y se ponen en contacto con los posibles compradores.

Según se explica en el informe de G Data, una de las plataformas principales de estos círculos son los foros de discusión, también llamados boards, donde los principales asuntos son los botnets, spam, sustracción de datos, etc. El abanico ofertado va desde el foro para Script Kids, para quienes les gustaría jugar a piratas de la red, hasta otros boards conocidos y temidos en que se comercia con datos de tarjetas de crédito, objetos robados y muchas otras mercancías. Estos boards tienen claramente un objetivo criminal. Los autores de la investigación destacan que cuando más ilegal es el contenido del foro, mayor es también el esfuerzo realizado por los responsables para encubrirlo de los lectores no invitados. Aunque por lo general la estructura de estos boards no es muy diferente de los foros normales. Con frecuencia solo hay una zona privada accesible únicamente a los miembros que forman el núcleo del equipo u otras personas que se hayan ganado la consideración de estos por servicios o merecimientos especiales. Todos los demás miembros solo pueden acceder a la zona pública normal del foro, pero también aquí se encuentran muchos datos útiles para los ciberdelincuentes en ciernes. De hecho allí los aprendices pueden encontrar mentores que, tras cobrar una considerable cantidad de dinero, les enseñan los secretos de este oscuro negocio. Por ejemplo, en este tipo de foros pueden figurar las instrucciones de instalación para la primera red propia de bots, vulnerabilidades actuales o Remote Administrations Tools (RATs). Los miembros expertos suelen también ofrecer a los novatos su ayuda a cambio de una remuneración. En ellos también contactan los vendedores y compradores de este mercado negro. Y en las salas privadas de estos foros, de acceso exclusivo para cibercriminales bien conocidos y de prestigio, se intercambian todo tipo de productos y servicios. Los principales acuerdos suelen hacerse fuera de los foros, a menudo a través de ICQ o canales IRC manipulados (dos sistemas de mensajería instantánea). Además cualquiera



que prefiera hacer negocios en un entorno todavía más profesional puede recurrir a una de las muchas tiendas online ilegales que existen. En ellas, los compradores pueden beneficiarse de importantes descuentos al adquirir grandes cantidades de datos robados e incluso se les devuelve el dinero si no quedan satisfechos con el servicio. Así por ejemplo, si los datos de tarjetas de crédito recién adquiridos no fuesen válidos ya –al haber cancelado el usuario legítimo dicha tarjeta-, se pueden reclamar otros datos o la devolución del dinero.

Principales servicios

Junto a los datos robados, existen otros servicios también muy populares, recoge el informe de G Data. Los principiantes suelen solicitar ataques DDoS, servicio que puede tener un precio de 10< por hora de ataque ó 50< por día. Además de hacer un buen precio, este tipo de servicio también se publicita, utilizando herramientas de marketing al uso como banners publicitarios. Los documentos de identificación - carnés de conducir o de estudiante falsificados, pero también los carnets y tarjetas de identidad robadas- son una mercancía muy solicitada también puesto que son documentos que ayudan a ocultar la propia identidad o suplantar una ajena son objeto de la interés. Según las investigaciones de G Data, especialmente en los foros clandestinos rusos prospera un comercio floreciente con estos documentos. La documentación falsificada o robada también es muy útil a la hora de abrir cuentas que luego se utilizarán como punto de pago para el botín robado. Para registrarse en los casinos online o en las casas de subastas suele necesitarse casi siempre documentación personal de identificación.

Otro servicio muy demandado lo constituye la denominada 'dropzone'. Existen tanto en el mundo virtual (un servidor en el que, por ejemplo, pueden depositarse copias ilegales de obras protegidas por la propiedad intelectual o incluso pornografía infantil) como en el mundo real (una dirección para la entrega de productos que han sido comprados con datos de tarjetas de crédito robadas). En un caso los hostings a prueba de balas se ocupan de todo; en el otro, mucha gente ofrece su dirección para recibir los bienes comprados fraudulentamente –por supuesto, a cambio de una buena tarifa. Los proveedores del 'hosting blindado' proporcionan a sus clientes una sede de servidores a salvo de la actuación de las brigadas internacionales de investigación. En el libro blanco 2009 "La economía sumergida" se recoge que el nombre más conocido en este negocio es el de la red Russian Buiness Network (RBN) o también el hoster americano McColo. McColo ya ha sido apartado de la red pero RBN sigue en activo con numerosas pequeñas filiales. Allí los ciberdelincuentes encuentran un refugio para entregar los datos de sus redes de bots, regentar sus tiendas online ilegales, alojar con seguridad sus servidores C&C (Command & Control) y un largo etcétera. Una zona de descarga está constituida por un servidor al que, por ejemplo, el spyware enquistado en un ordenador puede transferir los datos capturados en el ordenador de su víctima. La cartera de productos abarca desde los proveedores serios con una oferta reducida de espacio web, pasando por los servidores virtuales hasta los cúmulos de servidores, en función de las necesidades y de la capacidad financiera de cada uno.

Las condiciones de uso de estos proveedores tienen una formulación más bien artificiosa que a veces no se encuentra el punto 'prohibiciones y comportamientos indeseados'. La oferta es amplia e incluye desde copias piratas hasta proveedores que incluso dan hospedaje en sus servidores a contenidos pedófilos. También es larga la lista de países en que se ofrecen estos servicios, así se encuentran con frecuencia ofertas cuyos servidores están emplazados en Rusia, Turquía o incluso en Panamá. Un gran problema al que se enfrenta esta sociedad del crimen virtual es que, al registrar un dominio en los proveedores normales de hospedaje se guardan datos en la base de datos pública a la que pertenezca el dominio. A través del servicio Whois se podría averiguar información como el nombre, la dirección, el número de teléfono y la dirección de correo electrónico. Para evitar que su identidad que de al descubierto, los proveedores de hospedaje blindados camuflan estos datos, registrando los datos



de testaferros en el extranjero, preferentemente de África, pero también del área asiática. De este modo, el usuario de una oferta de hospedaje blindado está a salvo de que se llegue a conocer su identidad.

Otro servicio blindado llamado 'bulk e-mail' permite enviar por vía del servidor del proveedor correos electrónicos en masa, lo que se conoce como correos basura. Con frecuencia en la publicidad de estas empresas se afirma que los correos electrónicos que envían sortean los filtros antispam y llegan realmente a los ojos de los usuarios. Además, algunos proveedores tienen disponibles directamente las listas de direcciones de correo electrónico adecuadas, previo pago de una módica suma. Los titulares de estos servicios se suelen recorrer los principales foros de los bajos fondos virtuales para hacer publicidad allí de sus ofertas.

Robo de datos

Una gran parte del tráfico de datos robados de tarjetas de crédito, cuentas de PayPal o de eBay se desarrolla en las zonas de negocios en los boards. Pero también hay foros que se dedican exclusivamente a comerciar con mercancías robadas. Las ventas se contratan en zonas especialmente creadas con este fin dentro de los foros llamadas 'mercado negro' o, simplemente, 'mercado'. Según se explica en el informe de G Data, el procedimiento es el siguiente: alguien pone en venta una mercancía, como por ejemplo uno o varios ítems de eBay, indicando cuánto dinero exige por cada cuenta. A veces, incluso, el vendedor ofrece un descuento por cantidad si el cliente está dispuesto a adquirir todos o varios objetos del lote. Casi siempre, los potenciales compradores se presentan con una respuesta en el forum o establecen contacto directamente con el comprador utilizando los datos que este haya mencionado, para llevar a término el negocio.

La oferta comercial de la cibereconomía sumergida es muy variada: se demandan informaciones para crear cuentas, usurpar identidades o realizar toda la serie de tareas o acciones. El abanico abarca desde los datos personales, como son el nombre, la dirección, etc. hasta los datos bancarios y volcados de memoria de las bases de datos con cientos o miles de datos de usuarios. Los volcados de bases de datos se refieren a las copias de las bases de datos de las tiendas en línea o de los foros que tienen en su memoria los datos de los usuarios. En ciertos casos, estos datos se publican gratuitamente en estos foros piratas. Pero esta actuación suele limitarse a las bases de datos de otros boards porque este tipo de información obtenida en las tiendas online puede tener un gran valor en la economía sumergida.

Precios en el mercado negro

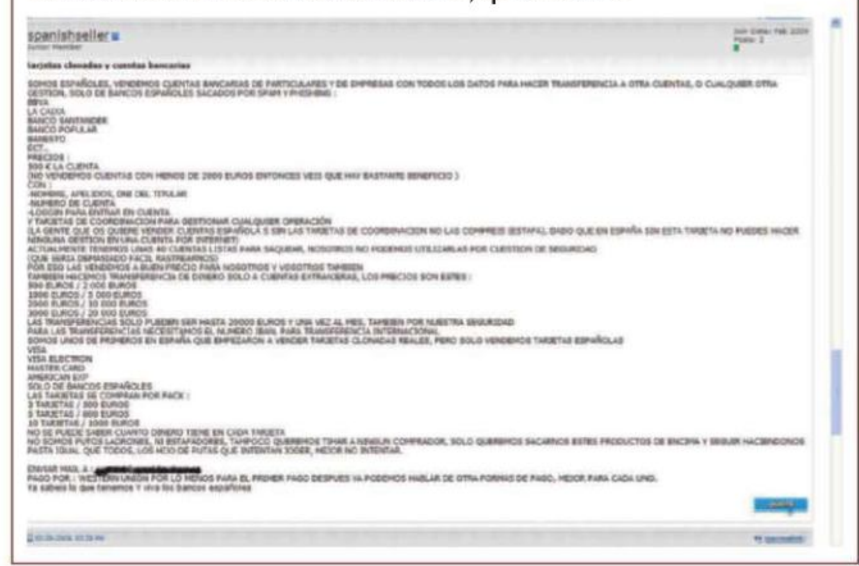
Producto/Servicio	Precio mínimo	Precio máximo
Ataque DDoS (por hora)	10.00 €	40.00 €
1 millón de correos basura dirigidos a las direcciones especificadas (por ejemplo, las cuentas de gamers)	300.00 €	800.00 €
Datos de tarjetas de crédito	2.00 €	300.00 €
Cuenta DHL pack station (precios basados en el volumen de datos disponible)	50.00 €	250.00 €
DNIs y carnets de conducir falsos (depende de la calidad de la falsificación)	50.00 €	2,500.00 €
Bases de datos con información personal (precios basados en el tamaño y el nivel de detalle)	10.00 €	250.00 €
Cuentas PayPal	1.00 €	25.00 €

Fuente: Libro blanco 2009 "La economía sumergida" elaborado por Marc-Aurél Ester y Ralf Benzmüller de G Data.

Las direcciones de las llamadas 'tiendas de tarjeta fácil' están también muy solicitadas. Se refieren a las tiendas en que los timadores informáticos pueden comprar con facilidad productos con los datos de tarjetas de crédito robadas porque la tienda no comprueba los datos. Cuantos más datos exija una tienda, mayor será el volumen de información que tendrá que comprar o capturar el hacker. Por eso los registros de datos de las tarjetas de crédito tienen un valor directamente proporcional a su integridad.

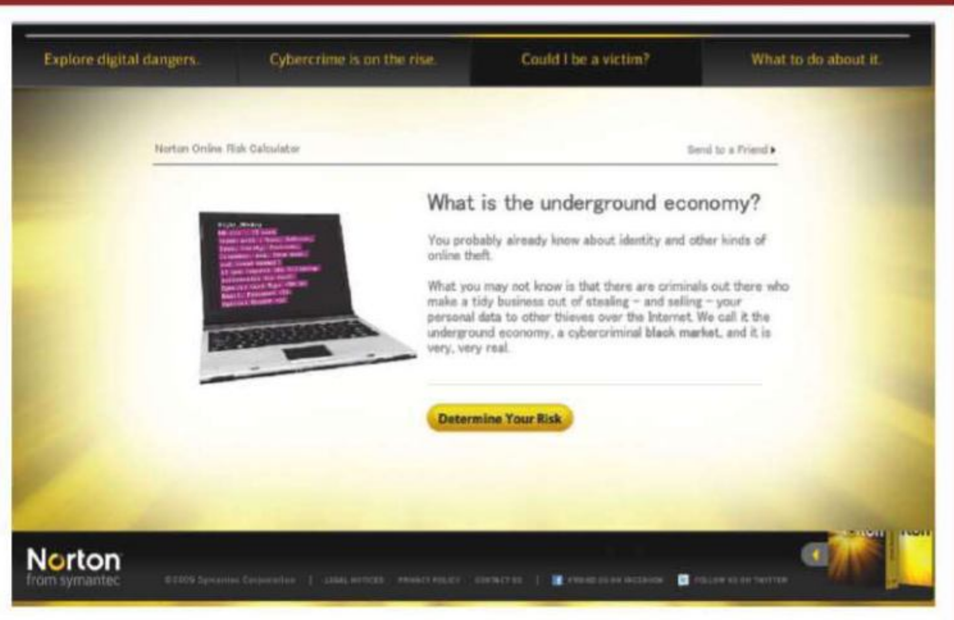
>>> PRECIO DE TARJETAS DE CRÉDITO

PandaLabs ha descubierto una red de ciberdelincuentes españoles dedicada a la venta en el mercado negro de cuentas bancarias de bancos españoles. A cambio de 500€, facilitan al comprador todos los datos necesarios de la víctima - nombre y apellidos, DNI, número de cuenta, nombre de usuario y contraseña- así como los datos de la tarjeta de coordenadas, utilizada por la mayor parte de los bancos españoles como una medida de seguridad adicional para evitar el fraude. Garantizan un saldo mínimo de 2.000 € en cada cuenta. También ofrecen como servicio realizar la trasferencia desde la cuenta robada, siempre que el destino sea un país extranjero. En este caso los precios varían, desde 500 € por realizar una transferencia de 2.000 €, hasta 3.000€ a cambio de una transferencia de 20.000€.
Para finalizar el abanico de ofertas, clonan todo tipo de tarjetas de crédito (VISA, Mastercard, American Express, etc.) asociadas también a cuentas españoles. Las venden por packs, desde 3 tarjetas a 500 € hasta 10 tarjetas por 1.000 €.
"Hoy en día es muy común el tráfico de datos de tarjetas de crédito; en este caso lo que más nos llamó la atención en un principio fue el precio, ya que normalmente este tipo de información se puede encontrar por 10 veces menos. Al ver el detalle de la oferta comprendimos el por qué del alto coste: al garantizar un saldo mínimo pueden aumentar el precio ya que las ganancias del comprador están aseguradas", explica Luis Corrons, Director Técnico de PandaLabs. "El 90% de los pagos derivados del robo de información bancaria se realizan siempre a través de Western Union, debido a lo fácil que es realizar transferencias de dinero a través de este sistema", apunta Corrons.



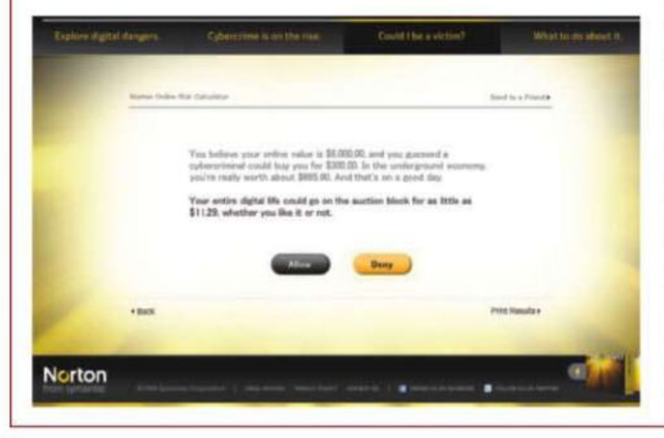
>>> VÍDEOS DEL MERCADO NEGRO DIGITAL

Los ciberdelitos superan al tráfico de drogas ilegales como actividad criminal para obtener beneficios económicos, según US Department of Treasury. De hecho, según Consumer Reports, una de cada cinco personas será víctima de este tipo de acciones. Cada tres minutos y medio se comete un delito en las calles de la ciudad de Nueva York y cada dos minutos y medio se comete un delito en las calles de Tokio, pero cada tres segundos alguien se apodera de la identidad de un usuario en la Red, esto supone cerca de 10.512.000 identidades cada año.



El ciberdelito es una actividad delictiva real, resulta más rentable, ofrece más anonimato y puede ser más difícil de perseguir que los delitos que se realizan offline. Symantec también está mostrando los trabajos más secretos de uno de los sectores ilegales más grandes del mundo, además de ofrecer al público la información que necesita para protegerse, proporcionando un conjunto de herramientas educativas así como una serie de iniciativas entre las que se incluyen el sitio web 'Todos los clics importan (Every Click Matters)', que examina los ciberdelitos de forma entretenida y educativa, explorando los peligros digitales y quién se encuentra detrás de estas acciones, para darle a conocer al usuario si puede verse afectado por un ciberdelito y educándole para saber lo que tiene que hacer si ha sido víctima de una de estas amenazas.

Asimismo Symantec ha colgado en YouTube una serie de videos sobre el Mercado Negro en Internet con el objetivo de invitar al público en general a realizar un tour virtual para saber cómo funciona el mercado criminal online, lo que allí se vende y los planes más recientes de los ladrones cibernéticos. En el video 'El Mercado Negro – El lugar donde se compran y venden identidades' disponible en http://www.youtube.com/watch?v=qLOEl7Z1PVs se ofrece una bienvenida oficial al mercado negro en Internet y le presenta cómo los ciberdelitos compran, venden, intercambian y comercian con la información confidencial de los usuarios – tanto los datos de las tarjetas de crédito como los números de la seguridad social, la información de cuentas bancarias, las contraseñas, las claves de acceso, los nombres de soltera de las madres de los usuarios,



la fecha de nacimiento o los números de teléfonos- es decir, cualquier dato que se pueda vender para obtener beneficios económicos.

"En la parte central de este tema se encuentran los ciberdelincuentes que están haciendo una fortuna en la Red y las víctimas que dejan a su paso. Estamos lanzando esta iniciativa porque sabemos que la educación puede hacer un gran trabajo para ayudar a las personas a entender los pasos de sentido común que deberían dar para protegerse," afirmó Rowan Trollope, vicepresidente primero de Consumer Products and Marketing en Symantec.

En 'La Fábrica de las Amenazas – Registro de las Teclas Pulsadas por las Víctimas y las Perspectivas de los Ciberdelincuentes' disponible en http://www.youtube.com/watch?v=SGZp4FeeNSk se ofrece una perspectiva única de las amenazas online, desde el punto de vista de los ciberdelincuentes, para mostrar cómo realizan sus engaños. En 'La Fábrica de las Amenazas - Phishing para las víctimas', disponible en http://www.youtube.com/watch?v=GqD3nrHJfn8, se dan a conocer los engaños que utilizan técnicas de phishing mediante mensajes spam, sitios web malintencionados, mensajes de correo electrónico y mensajería instantánea para hacer que los usuarios proporcionen información confidencial como, por ejemplo, datos de cuentas bancarias y números de tarjetas de crédito.

Finalmente en 'Principales ciberdelincuentes y estafadores' disponible en http://www.youtube.com/watch?v=jy3bev_Ykfw, se descubre a los principales estafadores que realizan sus delitos online y se explora algunos de los más recientes planes que utilizan para apoderarse del dinero de los usuarios.

Otra de las iniciativas puestas en marcha por el fabricante es una calculadora de riesgos online que ofrece Norton para proporcionar al internauta una herramienta rápida y gratuita para evaluar su nivel de riesgo y ofrecerle un valor estimado de sus datos personales para los ladrones que operan en el entorno criminal. En http://www.everyclickmatters.com/victim/assessment.html se puede realizar en tan solo dos minutos esta encuesta. Tras realizarla, a modo de prueba, contestando spreguntas sobre hábitos de compra online, límites de saldo de tarjetas bancarias y disponibilidad en la Red de información personal, hemos obtenido un valor de 695 dólares. Más de el doble de lo que servidora, humildemente, había estimado al inicio de la encuesta.

En la cibereconomía sumergida la mayor parte de los implicados tienen interés en encubrir los datos que pudieran dar pistas sobre su verdadera identidad, por lo que es imprescindible recurrir a los servicios proxy. Así, los ciberdelincuentes evitan que sus direcciones de IP acaben registradas en los protocolos. No en vano, estos protocolos podrían convertirse mañana en objeto de pillaje y - no sería nada extraordinario - estos datos de usuario acabarían publicados luego en otro lugar. Por eso, el usuario envía sus consultas al servidor proxy y éste coloca por orden del usuario la consulta, por ejemplo, en un foro; en los protocolos y registros del foro figurará únicamente la dirección IP del servidor proxy y no la del usuario. Con este método no se puede determinar a posteriori la dirección IP que tenía este usuario. Otro servicio también muy demandado es la protección anti DDoS que ampara a los clientes ante los ataques de sobrecarga. Esta precaución no está de más porque las rivalidades en este submundo cibernético están a la orden del día, y con ellas los ataques de denegación de servicio.

Hacerse con el botín

Según el Libro Blanco de G Data "La economía sumergida", la enorme variedad de herramientas y procedimientos confluye luego en una sola e idéntica meta: los criminales lo que quieren es ganar dinero. La paradoja es que el mayor problema con el que se enfrentan es cuando ya tienen el botín en su poder. Hay muchas formas de proceder para el 'cashout' o conversión en efectivo legal. En este 'cashout' se trata de convertir el dinero virtual en dinero real blanqueado, sin que se pueda luego rastrear su procedencia. En muchos casos, con los datos robados de tarjetas de crédito o también con el pago virtual que el ciberdelincuente ha recibido por expedir spam, se compran mercancías en Internet. Para que no les apresen al recibir la mercancía, las compras se envían a 'dropzones' o lugares neutrales de entrega. Allí tienen testaferros, que también suelen servir de correos o de expertos en logística en los envíos de e-mail, para reexpedir las mercancías con toda celeridad. Las 'dropzones' tienen por eso mucho éxito y por eso en las plataformas al margen de la legalidad, se ofrecen numerosos servicios de esta clase. La forma de proceder sigue siempre el mismo esquema. La mercancía se pide y se hace enviar a una dirección en Rusia o en otro país donde es recogida de la oficina de correos y reexpedida a la dirección de destino auténtica. El testaferro se hace pagar generosamente por su trabajo, a veces en especie, porque se pide también mercancía para sí mismo. Se han utilizado con estos fines casas y pisos deshabitados, llamados entonces en la jerga hacker inglesa 'house drop'. A una dirección fija de estas características puede uno también recibir correo de los bancos. Los cambios de dirección necesarios suelen poder realizarse en línea pero otra forma de alcanzar el mismo resultado es que el timador vaya al banco y le pida a un amable empleado que cambie la dirección. Los documentos falsificados necesarios para esta operación puede adquirirlos por un módico precio en el mercado negro correspondiente. Si además tiene nervios de acero y sabe convencer a los demás de sus mistificaciones, sus 'house drops' serán un éxito. Para mover el dinero en los casinos online se puede ingresar, por ejemplo, con la cuenta de PayPal robada. Por supuesto, el ciberdelincuente no se registra con su verdadero nombre sino con datos falsificados. Así por ejemplo, en los foros de este inframundo ilegal hay listas en que se valoran los portales de las casas de apuestas deportivas y casinos según su idoneidad para los tejemanejes criminales. Es decir, desde el punto de vista de si las empresas solicitan muchos datos para crear una cuenta, si comprueban con cuidado la autenticidad de los datos o si aceptan copias manipuladas de los carnés de identidad. Por eso son tan apreciadas las cuentas robadas que ya habían sido verificadas antes. Desde allí las remesas de dinero siguen su viaje, preferentemente a un 'bank drop', término que se refiere a una cuenta a la que los ciberpiratas tienen acceso pero de la que no son titulares. No es de extrañar que en la economía sumergida se vendan verdaderas guías de instrucciones para hacerse con una cuenta anónima para sumas importantes. Las ideas propuestas van desde sobornar a un empleado de correos para poder abrir una cuenta que normalmente se verificaría mediante el sistema de identificación postal hasta comprar documentación personal falsificada con la que abrir luego una cuenta. El sistema de identificación postal requiere que el interesado se persone con su documentación en una oficina del servicio de correos de turno. Una vez allí, el empleado de correos comprueba la documentación y reexpide la verificación al banco donde se desee abrir la cuenta. Con frecuencia se combinan varias de estas posibilidades.

Varios frentes

A modo de conclusión, los autores del informe de G Data Security Labs, Marc-Aurél Ester y Ralf Benzmüller, destacan que ya son prehistoria los tiempos en que el mundo hacker estaba habitado por jóvenes inmaduros que daban golpes de efecto en la red por diversión e interés en la tecnología. Por eso, para la generación actual que se mueve como pez en el agua en la cibereconomía sumergida ya no se ajusta ni merece la denominación 'hacker'. Se trata más bien de delincuentes de guante blanco con conocimientos técnicos. En este mundo al margen de la legalidad todo gira en torno al dinero y en él se mueven anualmente millones ya sea por robo directo a personas o mediante correo basura. Los malhechores suelen organizarse en bandas con estructuras profesionales en que cada cual está encargado de una tarea definida. Para el usuario delante de su ordenador esto significa que cada vez es más importante proteger su ordenador de las malas compañías. "Quién, a día de hoy, navega por Internet sin una solución efectiva de antivirus y cortafuegos está totalmente expuesto a convertirse en una víctima más de estos criminales. Justo en nuestra época, en que las casas de subastas en línea y la banca online forma parte de la vida cotidiana, este comportamiento conlleva un riesgo considerable", remarcan. Otro tema importante es el trato dispensado a sus datos personales. Muchos, sin pensárselo mucho, escriben toda serie de datos personales en su perfil de la red social, sin tener en cuenta que con ello están dejando una serie de bazas en las manos de los cibertimadores. Y es que incluso información aparentemente trivial como la fecha de nacimiento puede permitir a los estafadores completar los datos de la tarjeta de crédito. Según señalan los autores de este libro blanco de G Data, un fenómeno que parece que va camino de convertirse en tendencia es que los ciberdelincuentes le roben a alguien del ordenador los datos de la cuenta de su página web para luego utilizarla con oscuros fines. Por eso, los proveedores de soluciones de seguridad advierten que, en caso de una infección, se compruebe también sin falta la página web que uno tenga no solo el ordenador.



FRIKI GADGET



Medion de altas prestaciones

Ya seas diseñador, jugón, cinéfilo o editor de vídeo… Medion tiene la solución para todos aquellos que requieran de un equipo de altas prestaciones para gestionar su trabajo. Se trata del potente y novedoso PC 7192 que ofrece todas las ventajas técnicas que necesitas para sacar el máximo partido a tu vida multimedia. Cuenta con un procesador Intel Core i7 – 920, que dispone de velocidad de procesamiento de 2,66 GHz, ofreciendo un mayor rendimiento y un menor consumo energético. Además, dispone de 12 GB de memoria RAM y 1,5 TB de disco duro. Además viene equipado con el nuevo sistema operativo Windows 7 de Microsoft. Incorpora también una tarjeta nVidia GeForce GT230. La unión del procesador Core i7 con el nuevo Windows 7, a través de la API DirectComputer de Microsoft, es una de las características más relevantes en cuanto a aprovechamiento del procesador gráfico, utilizándolo para acelerar los gráficos y las operaciones de cálculo. Cuenta también con un sistema de conexión LAN 10/100/1000 Mb con el que podrás competir online con otros jugadores y un sistema de sonido de ocho canales para que no pierdas ni un solo detalle en tus partidas. El nuevo equipo de Medion incluye DVD grabador, tarjeta de sonido de ocho canales, salidas para micrófono y auriculares, teclado inalámbrico, ratón óptico y antivirus gratuito a 90 días. **www.medion.es**

Altavoz por vibración

Los altavoces Stridor, creados por Tacen, llegan de la mano de Sistemas Ibertrónica para ofrecernos el sonido más nítido mediante un procedimiento muy llamativo. Y es que los nuevos Stridor tienen la facultad de transmitir las ondas sonoras por toda el área de la superficie sobre la que se colocan. De este modo, al reproducir música o cualquier otro tipo de archivos de audio y colocarlos sobre una mesa, los usuarios podrán experimentar cómo la mesa se transforma en un gran altavoz. Cada superficie creará un tipo distinto de efecto sonoro durante la reproducción. Estos amplificadores se presentan en color negro para encajar en todo tipo de escritorios y no ocupar demasiado espacio en ellos, gracias a sus reducidas dimensiones - 60x60x45,5 mm - y su peso de 300 gr. Los altavoces Stridor han sido especialmente diseñados para los usuarios de portátiles. Y, además, son compatibles tanto con PC como con MAC. Su uso e instalación es muy sencillo, ya que se tratan de dispositivos 'Plug&Play' que sólo requieren conectarse al equipo a través de un puerto USB. **www.ibertronica.es**



Monitores ThinkVision ecológicos

Lenovo ha presentado cinco nuevos monitores de su gama ThinkVision que promueven el diseño ecológico y la facilidad de uso con un gran rendimiento visual. Entre los nuevos equipos presentados, destaca el monitor panorámico ThinkVision L2251x, el más respetuoso con el medioambiente de la compañía gracias a su bajo consumo energético, la utilización de plásticos reciclados en su fabricación y por ser el primer monitor de PC de la industria que ha conseguido la certificación TCO Certified Edge. Los nuevos ThinkVision L1711p, L1951p panorámico, L2250p panorámico, L2251p panorámico y L2251x panorámico han obtenido la certificación TCO Certified Edge, la clasificación EPEAT Gold y son un 50% más eficientes que los modelos anteriores, superando los criterios de la Energy Star 5.0. **www.lenovo.com/es**



dot m/u, un netbook con personalidad de portátil

En NightSky Black (negro cielo nocturno) y Cherry Red (rojo cereza), el dot m/u de Packard Bell combina una tapa brillante con unos interiores opacos con detalles cuidados. Ideal para quien duda entre los pequeños y manejables netbook y las prestaciones de los ordenadores portátiles, el dot m/u de Packard Bell es el primer netbook del mercado capaz de ofrecer las prestaciones de un ordenador portátil. Su pantalla de 11,6", su formato 16:9 y su tamaño reducido (menos de una pulgada de grosor y sólo 1,40 kg de peso) ofrecen una excepcional portabilidad sin comprometer la calidad de visión. Sutil y ligero, ultracompacto como toda la línea de netbooks dot de Packard Bell, el nuevo dot/mu es capaz de ofrecer hasta 8 horas de duración de la batería, una enorme facilidad de uso, una conexión constante a Internet (lleva incorporado todo lo necesario para chatear y la conexión a la red social) y un entretenimiento de alta definición. **www.packardbell.es**

Nuevo marco digital-reloj/despertador-radio

El HANNspree SG4311SB es un marco-reloj/despertador y radio con pantalla de LCD de 4,3", diseñado en color negro brillante con cristal acrílico biselado. Este dispositivo, con unas medidas de 123,55 x 91,83 x 33 mm, destaca por su diseño y facilidad de uso; precisamente, su moderno diseño y funcionalidad le han valido el Good Design Award 2009. El modelo SG4311SB ofrece una resolución de imagen de 480x272 píxeles permitiendo visualizar cómodamente sus fotografías así como disfrutar con la programación radiofónica o reproducir los últimos hits musicales, sin olvidar sus funciones adicionales de reloj despertador y calendario. Reproduce archivos en formato JPEG, BMP, MP3 y WAV y cuenta con múltiples ángulos de visualización (150º/130ª) para una total libertad de uso. Incorpora un altavoz de 1W de potencia, salida de auriculares y un puerto USB 2.0. Dispone de varios tonos de alarma a elegir, función día/noche así como modo slepp/snooze. **www.hannspree.com**





WD TV Live HD con conexión de red

Este reproductor multimedia de WD, que incorpora conexión de red y resolución Full HD 1080p, reproduce fácilmente vídeos HD (Alta Definición) almacenados en discos USB y de red, así como contenidos de Internet de sitios web populares, en la mayor pantalla de su hogar: su televisor HD. Creado a partir del exitoso reproductor multimedia WD TV HD, el WD TV Live HD ofrece una nueva interfaz más amigable que ayuda a los consumidores a disfrutar de un mundo de contenidos digitales en su salón, sin necesidad de ordenador. La conexión de red del reproductor multimedia WD TV Live permite a los usuarios transmitir o transferir películas desde un ordenador Windows o Mac o un dispositivo de almacenamiento en red (como los discos de red WD My Book World Edition y WD ShareSpace) a sus televisores HD. El reproductor multimedia WD TV Live también permite transmitir contenidos completos desde YouTube, Flickr y Pandora. **www.westerndigital.com**

FRIKI GADGET



Syclone: la caja más radical para gamers

Los gamers vuelven a convertirse en protagonistas del catálogo de Sistemas Ibertrónica. Para ellos, se lanza ahora la nueva caja Syclone, todo un portento de chasis en el que convergen un diseño rompedor - lleno de brillos, luces LED y colores en su parte frontal inspirado en las naves espaciales de películas de ciencia ficción - y las mejores ventajas del mercado para configurar un gran equipo informático. Su interior, pintado totalmente en negro (o gris metálico, según modelo), ofrece un amplio espacio para realizar el montaje de todo tipo de componentes, sin necesidad de utilizar herramienta alguna para el montaje de las unidades. Entre las opciones, destacan las cuatro bahías externas para unidades de 5'25"; dos externas para las de 3'5" y otras cinco bahías internas para 3'5". A ellas, hay que añadir siete slots de expansión y un rack para el disco duro que puede girarse 90º grados para una óptima instalación. Su estructura aerodinámica ha sido diseñada para garantizar un excelente flujo de aire. Para reforzar esta función, incluye dos ventiladores: uno trasero (o frontal, según necesidades) de 120mm y uno lateral de 140 mm. En el panel frontal que los usuarios podrán adquirir en negro, rojo o gris metalizado, se hallan sus puertos de conexión: dos USB 2.0 y uno e-Sata y audio (HD audio + AC97). **www.ibertronica.es**



Ventiladores controlados al máximo

Con el nuevo regulador ZM-MFC3 de Zalman es posible tener conocimiento en todo momento de las acciones que lleva a cabo el equipo informático. A través de su visualizador FSTN (visible desde múltiples ángulos), los diferentes indicadores nos informarán sobre: la carga de la fuente; el tiempo que lleva encendido el PC; la velocidad de los ventiladores (RPM) y la temperatura. El nuevo ZM-MFC3, distribuido por Sistemas Ibertrónica, ofrece la posibilidad de seleccionar hasta cuatro ventiladores/sensores distintos (ya sean con función RPM y PWM). Para elegir las revoluciones por minuto y el ventilador que se desea controlar, el usuario tan sólo tiene que girar la rueda que el regulador presenta en su frontal. Otro rasgo importante a destacar es el circuito de protección y alarma que lleva integrado. El ZM-MFC3 ocupa el espacio de una unidad de 5'25", con unas medidas: 147 x 87 x 42 mm. **www.ibertronica.es**



Vuelven LaCie y Philippe Starck

Quince años han pasado desde la primera colaboración de Philippe Starck con LaCie. Cuando parecía que todo estaba inventado en discos duros externos, vuelven a juntarse para marcar tendencia y aportar utilidades desconocidas hasta ahora. Así los discos duros se hacen táctiles: LaCie Starck es una nueva línea de discos de sobremesa y portátiles con una superficie inteligente. Capaz de abrir la aplicación deseada en función de si se toca brevemente o durante unos segundos. La gama de discos externos LaCie Starck incluye unidades de sobremesa, con más capacidad y unidades portátiles, para llevar en el bolsillo. LaCie Starck Desktop Hard Drive es la unidad de sobremesa que se ofrece con capacidades de 1 y 2 TB. En ambos casos son unidades que se conectan por USB 2.0 y sin necesidad de instalar ningún driver. LaCie Starck Mobile Hard Drive es la opción portátil para llevar en el bolsillo la información. En concreto, está disponible con modelos de 320 y 500 GB de capacidad. También en este caso se conectan por USB 2.0 y sin tener que instalar ningún driver en el ordenador. Todas las unidades de la nueva gama LaCie Starck incluyen los programas LaCie Backup Assistant y LaCie Desktop Manager que ayudan a formatear, hacer backups y personalizar el disco duro. **www.lacie.es**



Toshiba StorE TV, reproductor y centro de almacenamiento multimedia

Toshiba amplia su familia de productos StorE con el nuevo StorE TV, un disco duro multimedia con una capacidad superior a los 2 terabytes para almacenar y reproductor películas, música y fotos. El dispositivo tiene un diseño sencillo en negro brillante y unas medidas de 170 x 46 x111 mm, lo que le convierte en un aparato muy discreto para cualquier entorno del hogar. El nuevo Toshiba StorE TV dispone de un disco duro de 3,4" (8.89cm), que proporciona una capacidad de más de 2 terabytes –suficiente para más de 770 horas de reproducción en calidad DVD. El dispositivo decodifica videos en definición de calidad estándar (por encima de 720 x 576) y es capaz de convertir contenidos SD a calidad HD (1080i), y reproducirlos vía HDMI en una televisión. StorE TV es compatible también con diversos formatos de música como MP3, WMA, WAV y AAC, así como decodificador de videos en formato JPEG. Otros interfaces del dispositivo permiten reproducir video, audio estándar y USB. El dispositivo también soporta especificaciones para clientes y host USB. **www.toshiba.es**

Fuentes de alimentación Straight Power E7

La nueva gama de be quiet! ha sido desarrollada para proporcionar la máxima eficiencia energética y se adapta a las necesidades de todo tipo de equipos, ajustando de forma constante la cantidad de energía suministrada a fin de reflejar la carga de trabajo a la que se enfrenta el PC en cada momento: desde los cerca de cero vatios en modo stand-by hasta el máximo soportado por la fuente trabajando con aplicaciones de gama alta. Las nuevas Straight Power E7 poseen la certificación 80Plus Bronce, con lo que se garantiza un consumo mínimo de energía y un alto nivel de eficiencia de hasta un 88%. La familia Straight Power E7 consta de nueve modelos distintos - disponibles con o sin cable de gestión- con una potencias de 400W, 450W, 480W, 500W, 550W, 580W, 600W, 680W y 700W. Estas fuentes de alimentación be quiet! están equipadas con cuatro raíles separados de 12V para proporcionar un suministro de energía estable a todos lo componentes del sistema, asegurando una alta fiabilidad. Además, están provistas de un PFC activo de menos del 0,9 a pleno rendimiento, permitiendo disfrutar de un suministro de potencia altamente estable. También destacan por su característico funcionamiento ultra silencioso gracias a la presencia de los ventiladores Silent Wings be quiet! de 120mm. Estos diseños son compatibles con los últimos estándares (ATX 12V versión 2.3 y EPS versión 2.92) y están fabricados para ofrecer una gran durabilidad de hasta 100.000 horas a 25ºC. **www.be-quiet.com**

Placas base X8SIE/ X8SIE-F, de Supermicro



Flytech amplía su gama de placas base creadas por el especialista Supermicro con la llegada de las nuevas placas base XSIE/ XSIE-F. Ambas plataformas de alto valor optimizadas para formato 1U se basan en el chipset 3420 de Intel y destacan especialmente por su bajo consumo energético, un rendimiento global mejorado y una excelente relación calidad/precio. Las placas X8SIE/ X8SIE-F consiguen una eficiencia VRM (Módulo Regulador de Voltaje) de más del 90%, lo que supone un incremento del 50% respecto a la anterior generación de servidores mono procesador. Los modelos X8SIE y X8SIE-F soportan procesadores Intel Xeon de la serie 3400 con socket LGA 1156, gracias a su diseño optimizado que cuenta con Controlador de Memoria Integrado (IMC). El procesador Xeon serie 3400 ofrece la posibilidad de trabajar con hasta dos canales de memoria DDR3 ECC con un máximo de 2 DIMMs por canal para 1333 y 1066, funcionando a 800MT/s. www.flytech.com.es. **www.supermicro.com**

Discovery 975 Bluetooth, con tecnologías de anulación de ruido

Plantronics ha presentado el Discovery 975 Bluetooth, el nuevo auricular que sustituye al Discovery 925 y que incluye las avanzadas tecnologías AudioIQ2 y WindSmart, que reproducen la voz natural en entornos muy ruidosos, además de comodidad, durabilidad y una excelente calidad de sonido para quien recibe la llamada. El Discovery 975 incorpora AudioIQ2, que funciona automáticamente cada vez que el usuario mantiene una conversación, y dos micrófonos para captar con precisión la voz del usuario y al mismo tiempo anular el ruido ambiental. Además anula el ruido causado por el viento con tecnología WindSmart, que incorpora una rejilla estriada en el micrófono y un tejido acústico que rodea al micrófono para protegerlo del viento. Asimismo, los filtros electrónicos dentro del AudioIQ2 eliminan el ruido producido por el viento durante las conversaciones y transmiten una voz clara y natural. El auricular incluye un ecualizador de 20 bandas adaptable que transmite una voz viva y clara y funciona con AudioIQ2, para ajustar automáticamente las llamadas entrantes a unos niveles de escucha cómodos basados en el nivel de ruido de fondo. **www.plantronics.com**

FRIKI GADGET



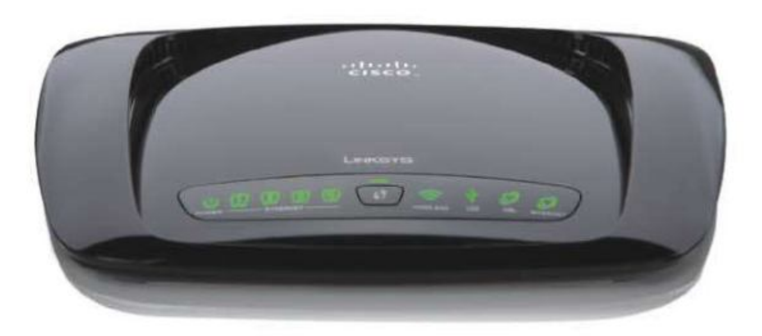
Nuevos iMac con pantallas de 21,5" y 27"

Apple ha anunciado una línea iMac completamente nueva con brillantes pantallas panorámicas de 21,5" y 27" con retroiluminación LED, con un nuevo diseño de cristal de borde a borde y con carcasa de aluminio uniforme. La nueva gama iMac incluye procesadores Intel Core 2 Duo a partir de 3,06 GHz y procesadores quad-core Core i5 e i7. Todos los nuevos iMac vienen de serie con teclado inalámbrico y con el nuevo ratón inalámbrico Magic Mouse, el primer ratón del mundo con tecnología Multi-Touch estrenada por Apple en el iPhone, iPod touch y en el trackpad de los portátiles Mac. El nuevo iMac incorpora una espectacular pantalla con retroiluminación LED y formato panorámico 16:9, ideal para ver películas en alta definición y series de TV, o para editar y ver tus propios vídeos y fotos usando iLife. **www.apple.com/es**



Home Base, de Belkin

En los hogares cada vez hay más ordenadores y con frecuencia es necesario añadir dispositivos a una red, algo que no tiene por qué resultar complicado con la tecnología adecuada. Consciente de esta necesidad, Belkin presenta su nueva Home Base, un dispositivo que se conecta inalámbricamente al router con tecnología Wireless-N y que permite acceder a todo los periféricos desde cualquier PC que esté conectado a la red en el hogar. Con los cuatro puertos USB de la Home Base es posible conectar discos duros externos para compartir música, fotos y vídeos con su familia. Además, podrá mantener los archivos a buen recaudo, ya que la Home Base hará copias de seguridad periódicamente de los ordenadores conectados en un disco duro externo y evitará así posibles pérdidas de datos. La Home Base también le permitirá acceder a lo archivos multimedia almacenados en discos duros conectados a una PS3 o Xbox 360. Sus funciones para compartir archivos le permitirán subir fotos a sus galerías de fotos online de Flickr o Picasa automáticamente. **www.belkin.com**



Gateway ADSL y Wireless-N de doble banda

Cisco anuncia el nuevo gateway Gigabit Linksys by Cisco con modem ADSL2+ y la última tecnología Wireless-N de doble banda (WAG320N) que proporciona una conectividad a Internet de alta velocidad. Con el módem ADSL2+ integrado, se puede conectar a una línea ADSL de alta velocidad y compartirla, lo que permite realizar transferencias de datos más rápidamente. La tecnología Wireless-N de doble banda permite seleccionar un espectro libre en entornos Wi-Fi saturados para que los usuarios puedan compartir una conexión a Internet de banda ancha con mayor velocidad y menos puntos muertos. Gracias al puerto StorageLink integrado, los usuarios pueden hacer que sus dispositivos de almacenamiento USB estén disponibles en la red doméstica, e incluso accesibles de forma remota a través de Internet. Además, el nuevo WAG320N incluye el Media Server que permite acceder desde cualquier reproductor doméstico compatible con UPnP a toda la música, vídeos y fotografías que estén disponibles.Network Magic permite configurar el WAG320N en cuestión de minutos. Además, ayuda a gestionar la red doméstica de forma segura, permitiendo ver qué dispositivos hay disponibles en la red conectados a Internet. **www.linksysbycisco.com**

OFERTA DE SUSCRIPCIÓN



Más fácil en www.mcediciones.com

Envía este cupón a:

MC Ediciones, S.A.
Passeig de Sant Gervasi, 16-20
08022 Barcelona

Precio ejemplar 4,95 euros
Suscripción España 44,55 euros
Suscripción Europa 103,95 euros
Suscripción resto mundo 163,35 euros.

☐ Deseo suscribirme a @rroba por un año (12 números) al precio especial de 44,55 euros

Según la ley 15/1999 de protección de datos personales, los datos que Vd. nos facilita serán incluídos en el fichero de MC Ediciones, S.A. para la gestión de la relación comercial con Vd. Los datos facilitados son estrictamente necesarios, por lo que su cumplimentación es obligatoria. Asimismo, Vd. consiente expresamente a MC Ediciones, S.A. para recibir comunicaciones comerciales de sus productos y servicios, así como de productos y servicios de terceros que puedan resultar de su interés. Vd. tiene derecho de acceso, rectificación, oposición y cancelación, que podrá ejercitar comunicándolo por carta a: MC Ediciones, S.A. (Paseo San Gervasio, 16-20, 08022 Barcelona).

Nombre y apellidos .... NIF o CIF ....

Dirección .... Teléfono ....

Población .... Provincia .... C.P. ....

Email ....

Para mayor comodidad puede suscribirse a través de nuestra web: www.mcediciones.com / suscripciones@mcediciones.com

FORMA DE PAGO

☐ Adjunto talón bancario

☐ Tarjeta de crédito

☐ VISA (16 dígitos) ☐ American Express (15 dígitos)

Tarjeta nº

Caducidad

Titular tarjeta o cta. cte.

Firma

☐ Domiciliación bancaria (Datos Banco/Caja)
Con renovación automática hasta su orden.

Banco o caja

Entidad oficina d.c. nº de cuenta

'Serial Experiments Lain', edición coleccionista

"Solo he abandonado mi cuerpo… En realidad sigo viva… Dios está aquí". Éste es el enigmático e-mail que recibe la tímida estudiante de 14 años Lain Iwakura de una compañera de clase. Esto no tendría mayor importancia, de no ser por el hecho de que la remitente del mensaje es Chisa Yomoda, una muchacha que acaba de suicidarse. A partir de ese momento, Lain pasará cada vez más tiempo conectada a la Red, obsesionada con la idea de encontrar una respuesta al increíble e-mail que parece estar relacionado con las muertes de estudiantes que se están produciendo a su alrededor. Poco a poco, Lain irá descubriendo que la línea que separa el mundo real y la Red ha comenzado a difuminarse y que nada es lo que parece, ni siquiera ella.

Dirigida por Ryutaro Nakamura con guión de Chiaki Konaka y diseño de personajes de Yoshitoshi Abe, 'Serial Experiments Lain' profundiza en la definición de la realidad tal y como la conocemos. La serie fue concebida originalmente para el anime por el joven productor Yasuyuki Ueda, que se esconde en los créditos bajo el pseudónimo de "Production 2nd". Su intención era desarrollar un proyecto personal que plasmara sus inquietudes de aquel momento: el drama de una adolescente, la influencia de las nuevas tecnologías en la sociedad y temas como la identidad y la realidad. El resultado fue el primer psico-thriller cyberpunk de la era de Internet, emitido originalmente en la cadena de televisión japonesa TV Tokyo en 1998.

Selecta Vision presentó en el Salón del Manga de Barcelona la edición coleccionista compuesta por 3 DVD que contienen los 13 capítulos de la serie, un DVD con extras, un CD con la banda sonora, un libreto integral, un manga y una litografía exclusiva de Yoshitoshi Abe. <



Karas

También en el Salón del Manga, Jonu Media aprovechó para lanzar Karas, serie que ha cosechado mucha expectación al combinar técnicas de arte en 2D y 3D. Es ganadora del 'Tokyo Anime Award' de 2006 como Mejor Vídeo Original. Tatsunoko Production (Speed Racer) realizó este esperado título para conmemorar su 40º aniversario en la producción anime.

Una guerra secreta está apunto de empezar en Shinjuku, Tokio, entre el demonio Eko y el yakuza Otoha. Eko y sus seguidores prefieren vivir en el reino humano, pero para ello deberán alimentarse mediante fluidos de cuerpos humanos. En una de sus masacres sobrevive una chica, cuyo padre, inspector de policía, se obsesionará por encontrar respuestas a las enigmáticas tragedias. Por su parte, Otoha (uno de los Karas) es, a su vez, un humano superpoderoso que puede transformarse en vehículo, avión y tanque blindado. Éste y otros personajes intentarán detener a su malvado predecesor Eko. <





Aurum distribuirá el catálogo de Studio Ghibli



Gracias a un acuerdo, Aurum Producciones distribuirá los grandes clásicos de Studio Ghibli en España. Entre 2009 y 2010 se va a editar en DVD los siguientes grandes clásicos de Studio Ghibli, totalmente remasterizados y en ediciones especiales: 'Nausicäa del Valle del Viento' ('Kaze no Tani no Nausicaä'); 'El Castillo en el Cielo' ('Tenkuh no Shiro Laputa'); 'Mi Vecino Totoro' ('Tonari no Totoro'); 'Nicky, La Aprendiz de Bruja' ('Mahou no Takyubin'); 'Recuerdos del Ayer' ('Omohide Poro Poro'); 'Porco Rosso' ('Kurenai no Buta'); 'Pompoko' ('Heisei Tanuki Gassen Ponpoko'); 'Susurros del Corazón' ('Mimi wo Sumaseba'); 'La Princesa Mononoke' ('Mononoke Hime').

Según informan desde Aurum Producciones aún se está definiendo junto con Studio Ghibli, los plazos y los contenidos de los que van a disponer, empezando a trabajar en nuevos doblajes, etc… por lo que no se puede anunciar ninguna fecha concreta.

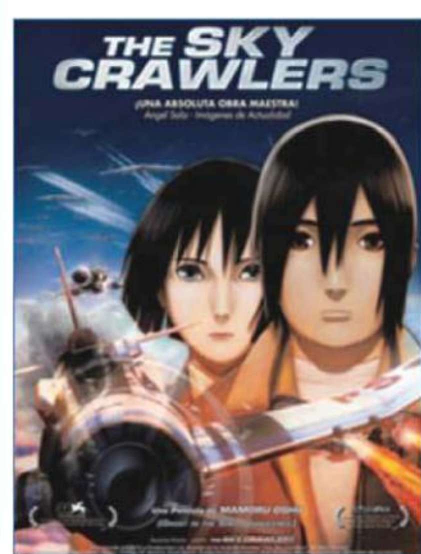
La relación entre Aurum Producciones y Studio Ghibli comenzó en el año 2006, cuando se estrenó la película El castillo ambulante, de Hayao Miyazaki. Posteriormente también se estrenó en cines 'Cuentos de Terramar', de su hijo Goro Miyazaki y, más recientemente, 'Ponyo en el acantilado', la última obra maestra del genial creador. En DVD se han editado también otros títulos emblemáticos como 'Mis vecinos los Yamada' y 'Puedo escuchar el mar'. Además, entre las muchas novedades que van a llegar a España está la primera edición en Blu Ray de una película de Studio Ghibli, 'Ponyo en el acantilado'. Y tras 21 años se ha estrenado en España en cines 'Mi vecino Totoro', una de las joyas de Miyazaki. No en vano el estudio adoptó el personaje como logotipo para sus producciones. <



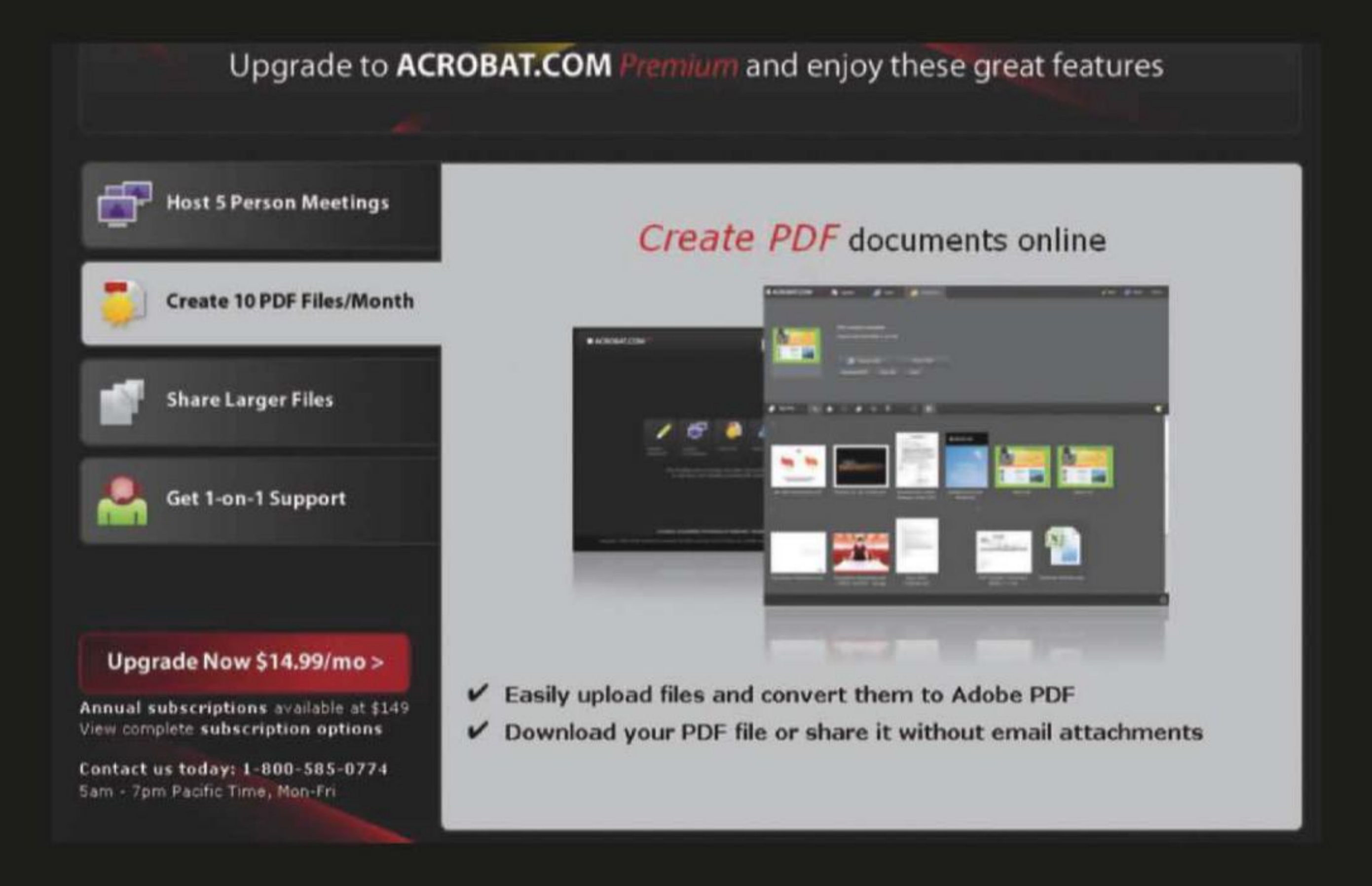
'The Sky Crawlers'

Vuela como si no existiera un mañana. Este es el lema de la película 'The Sky Crawlers', dirigida por Mamuro Oshii, autor también de la celebérrima 'Ghost in the shell', 'Innocence' y 'Patlabor'. Selecta Vision es la encargada de su distribución en España y previsiblemente se estrenará en cines también. De hecho los asistentes al Salón del Manga pudieron verla en la gran pantalla durante los cuatro días que duró el evento. 'The Sky Crawlers' está basada en la exitosa novela homónima de Hiroshi Mori, que cuenta con cinco volúmenes. En este film bélico de ciencia-ficción (que triunfó en Sitges 2008), se narra la historia de los Kildren, unos jóvenes pilotos que no crecen y cuya única misión es combatir. Pero todo ello con un enfoque metafísico y filosófico, como viene siendo habitual en sus producciones.

En 'The Sky Crawlers', Yuichi Kannami es traslado a su nueva base con tan solo unos vagos recuerdos de su pasado y la certeza de que ha nacido para pilotar aviones de combate. Pronto llama la atención de la comandante de la base Suito Kusanagi, que se comporta como si llevara mucho tiempo esperándole. La película cuenta con una evocadora banda sonora compuesta por el Maestro Kenji Kawai. Disponible en DVD y BlueRay, ambos formatos incorporan un especial 'Así se hizo'. <



Herramientas colaborativas on-line

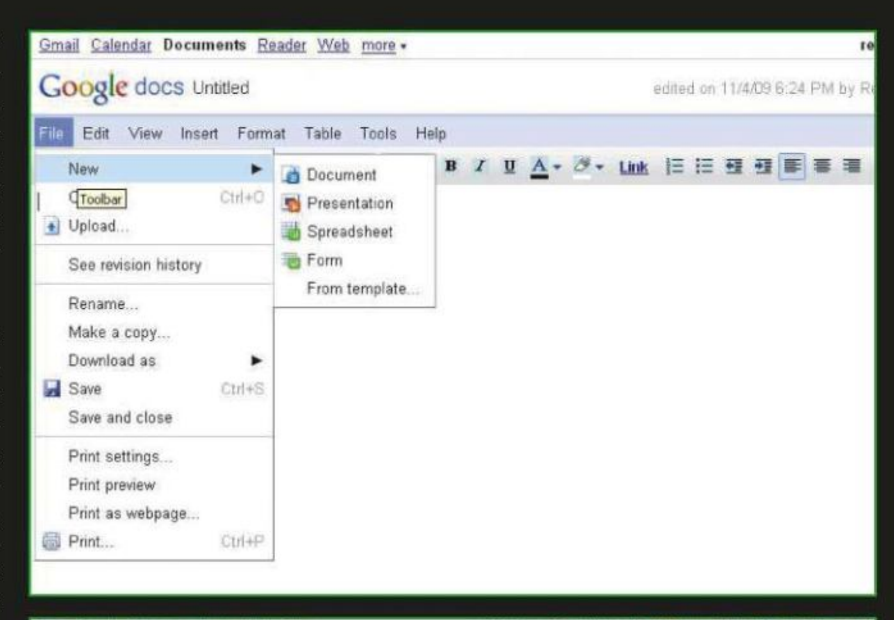


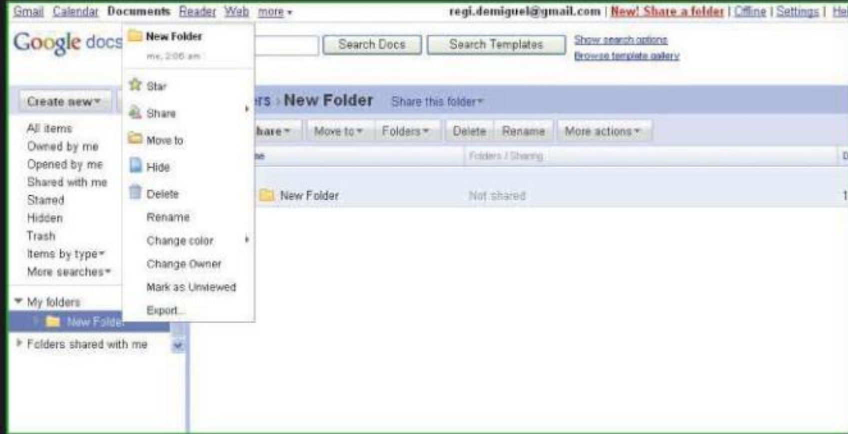
Hace tiempo que viene hablándose del "cloud computing", una tendencia que ha permitido que Internet no sólo sea un espacio que permite que los internautas busquen la información que necesitan. La red de redes también se erige como un espacio de encuentro en el que los usuarios pueden trabajar y compartir sus documentos de trabajo en un entorno on-line.

En el año 2004, Tim O´Reilly, conocido por sus trabajos para impulsar el software libre, acuñó un término que revolucionaría la idea y el uso que los internautas habían tenido de Internet hasta la fecha. Nacía la Web 2.0, concepto que se empleó para referirse a una concepción de Internet en la que las redes sociales, los blogs y los servicios pasaban a cobrar un papel fundamental. En este contexto, la nueva concepción de la Red tiene un enfoque colaborativo muy importante, sobre todo porque la tendencia hacía la que encaminamos nuestros pasos es un mundo virtual en el que todo está interconectado.

En un momento en el que la tendencia actual es trabajar con la Web, surge una pregunta casi obligatoria: ¿qué necesidad tiene una organización o un usuario particular de instalar un programa software en su equipo si existe la alternativa de recurrir a distintas herramientas on-line que están disponibles a través de Internet, y con el aliciente de que muchas de ellas son totalmente gratuitas? La respuesta a este planteamiento está ligada al concepto "de









la nube" y, en concreto, al software como servicio. Las ventajas que plantea esta nueva forma de desempeñar, por ejemplo, las típicas tareas ofimáticas son diversas aunque, quizás, la más importante (y evidente) tiene que ver con que las personas trabajan en un servidor web al que se conectan remotamente vía Internet.

Esto les va a permitir desempeñar sus actividades de manera mucho más cómoda, fácil y rápida porque, al no tener instalado ningún programa en su ordenador, el equipo va mucho más rápido y consume menos recursos. Otro aliciente de estas aplicaciones virtuales, también conocidas con el sobrenombre de cloudware, es su facilidad de uso. Eso sí, hay que cerciorarse de que se suben correctamente los documentos que necesitamos a Internet para que estén listos y sean accesible para aquellas personas que vayan a utilizarlos.

¿Y por qué cloud computing? Con el término de cloud computing, se hace referencia a la idea de informática en la nube. Se trata de un paradigma que permite ofrecer servicios de computación a través de la Web. En este caso, el usuario tiene acceso a un conjunto de discos duros virtuales, servidores y otros recursos, como por ejemplo programas, para que, precisamente, sean utilizados desde Internet y no desde el ordenador o el portátil. Así, el equipo se convierte en una especie de intermediario para acceder a las máquinas que ejecutan y guardan la información que se maneja en la Red.

A pesar de que estas propuestas son eficaces y efectivas, todavía no pueden sustituir a los programas de escritorio de toda la vida, ya que en ocasiones podemos encontrarnos con algunas carencias que se echan en falta. No obstante, con el tiempo lo más seguro es que algunas de las características de las que adolecen se irán mejorando y perfeccionando.

Google Docs

Una de las primeras firmas pioneras en este campo ha sido Google de la mano de su ya popular suite ofimática Google Docs. Es compatible con los navegadores web más conocidos (Internet Explorer, Opera, Safari, Firefox y Chrome) y llama la atención sobre todo por dos cosas. De un lado, su facilidad de uso (es posible organización en carpetas), lo que sin duda ayudará a las personas que nunca antes han utilizado una aplicación de estas características. De otro, la organización de los documentos de trabajo. Google Docs es completamente gratuito y está formado por las siguientes utilidades: Documents

ZOHO MAIL, ES UN SERVICIO DE CORREO ELECTRÓNICO QUE PERMITE TENER ACCESO AL E-MAIL INCLUSO SIN TENER CONEXIÓN A INTERNET O ZOHO PLANNER, UN COMPLETO ORGANIZADOR PERSONAL PARA QUE NUESTRA AGENDA PERSONAL ESTÉ SIEMPRE ACTUALIZADA.

>>> VENTAJAS Y BENEFICIOS

- **Puedes ganar mucho tiempo a la hora de trabajar, con la ventaja de tener un control sobre todos los documentos que manejas y consultar información siempre valiosa.**
- **Es posible definir los permisos que se asocian a cada uno de estos ficheros: sólo lectura o lectura y edición.**
- **Aunque desempeñar cualquier tarea en la nube significa conectarse a Internet, es posible obviar este requisito, siempre y cuando utilicemos las herramientas de edición de texto de Google Docs y Zoho Writer. Sólo se necesita instalar una extensión del navegador que se llama Google Gears. Gratuito y sencillo de manejar, una vez instalado en el ordenador se crea un acceso directo en el escritorio. Este programa tiene la capacidad de actualizar de manera automática los documentos tras restablecerse la conexión a Internet.**
- **Las suites ofimáticas virtuales están preparadas para compartir ficheros de trabajo en tiempo real, con la ventaja de garantizar su accesibilidad en cualquier instante y desde cualquier ordenador. Para acceder a estas herramientas, hay que registrase y especificar un nombre de usuario y contraseña.**

(para documentos), Spreadsheet (para hojas de cálculo) y Presentations (para presentaciones).

La propuesta de Google no sólo permite, por ejemplo, subir ficheros de texto o tablas de Excel que ya estén creadas a la nube para compartirlas y guardarlas on-line de manera segura, sino que también ofrece la opción de crear toda esta información desde cero y editarla de la misma manera que lo hacemos habitualmente con nuestra suite de medios ofimáticos: aplicar la negrita a una palabra, subrayar una frase, cambiar la fuente que estamos utilizando o modificar el color de las celdas de una tabla, entre otras posibilidades.

También existe la posibilidad de tener un control de las personas que queremos que vean y tengan acceso a nuestros documentos pudiendo, incluso, dejarles que incluyan sus propias ideas y comentarios. Así, es posible conceder varios permisos como lectura y escritura o sólo lectura (estos permisos se pueden modificar en cualquier momento en función de nuestras necesidades).

Google Docs está pensado para que





un máximo de 100 usuarios compartan el mismo documento, aunque el número de aquéllos que lo pueden editar simultáneamente se reduce a 10. El servicio, asimismo, posibilita monitorizar los usuarios que están conectados y quienes están llevando a cabo tareas de edición.

En función del tipo de archivo que se esté manejando, el peso de los ficheros varía: 500 Kb es el tamaño máximo para los archivos de texto y 2 Mb complementarios por cada una de las imágenes utilizadas. Por su parte, el peso de una presentación, ya sea un fichero con extensión .ppt o .pps, dependerá de la manera en que esta tarea se lleve a cabo.

Los archivos que se suben de Internet ocupan un máximo de 2 Mb y los del correo electrónico 500 Kb. En cambio, si esta presentación se decide subir directamente desde el propio ordenador el usuario tiene que saber que cómo máximo sólo puede subir 200 diapositivas ó 10 Mb. Y para las hojas de cálculo, cada una puede constar de hasta 200.000 celdas, 100 hojas ó 256 columnas, como mejor prefiera.

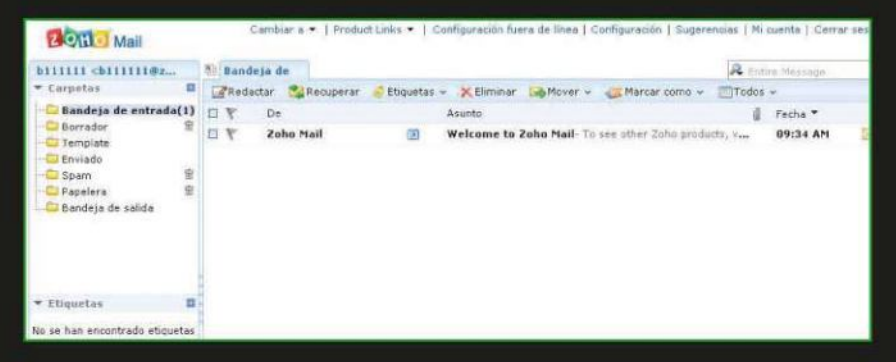
Zoho

Otra de las suites ofimáticas muy conocidas con la que es posible trabajar en la nube es Zoho, sin coste alguno. Su desarrollador es AdventNet y sólo se puede utilizar si nuestro navegador web es Firefox o Internet Explorer. Nada más abrir su página de inicio, el internauta se encuentra con un amplio y diversificado abanico de herramientas en las que no falta ni el editor de

>>> MICROSOFT SE LLAMA OFFICE LIVE WORKSPACE

Aunque en la actualidad Microsoft todavía no ofrece a sus usuarios una alternativa a su suite ofimática por excelencia, todo parece indicar que el año que viene (a lo largo del primer semestre) tendrá lugar el alumbramiento de dicha versión on-line de la mano de Office Live Workspace (http://workspace.officelive.es) para acceder a documentos on-line y compartirlos con otros usuarios, además de organizarlos y elaborar proyectos con independencia del ordenador en el que nos encontremos. Se podrán guardar más de 1.000 documentos, crear sencillas listas y notas web y compartir toda información en tiempo real. Las características más destacadas de Office Live Worspace son las siguientes:

- **Panel de Actividad: Muestra toda la actividad de un vistazo.**
- **Notificaciones: Los usuarios reciben notificaciones mediante e-mail acerca de los cambios realizados en sus espacios de trabajo o documentos.**
- **Subida de múltiples archivos: Permite subir diversos archivos a la vez arrastrándolos y soltándolos desde sus escritorios.**
- **Mejora de intercambios: La nueva funcionabilidad de intercambio incluye una interfaz de usuario más sencilla así como la capacidad de autocompletar las direcciones de correo electrónico.**



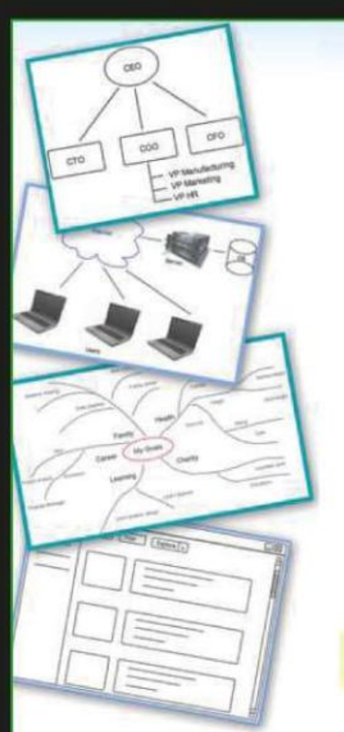
texto (Writer), ni las presentaciones (Show) ni las hojas de cálculo. Brinda, asimismo, otras alternativas no menos útiles e interesantes. Este es el caso de Zoho mail, un servicio de correo electrónico que permite tener acceso al e-mail incluso sin tener conexión a Internet o Zoho Planner, un completo organizador personal para que nuestra agenda personal esté siempre actualizada. Zoho provee de características bastante similares a las de Google Docs, pues permite crear desde cero un documento o trabajar con aquéllos que se suban a la aplicación directamente.

GOOGLE DOCS ES COMPATIBLE CON LOS NAVEGADORES WEB MÁS CONOCIDOS Y LLAMA LA ATENCIÓN SOBRE TODO POR SU FACILIDAD DE USO Y LA ORGANIZACIÓN DE LOS DOCUMENTOS DE TRABAJO.

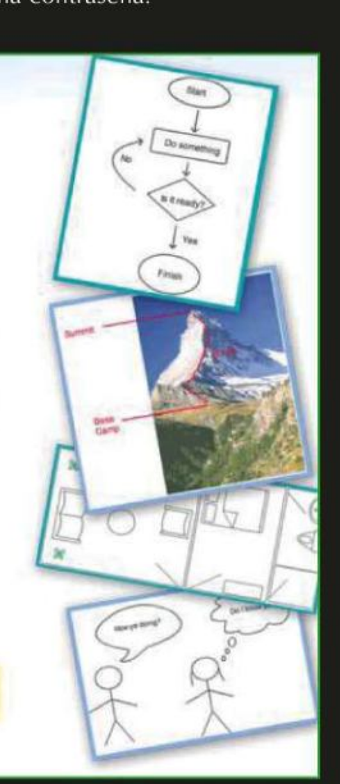
A diferencia del servicio de Google, está preparado para soportar archivos de mayor tamaño. Además, Zoho tiene la capacidad de importar archivos en formato Zip y proteger los ficheros mediante una contraseña.

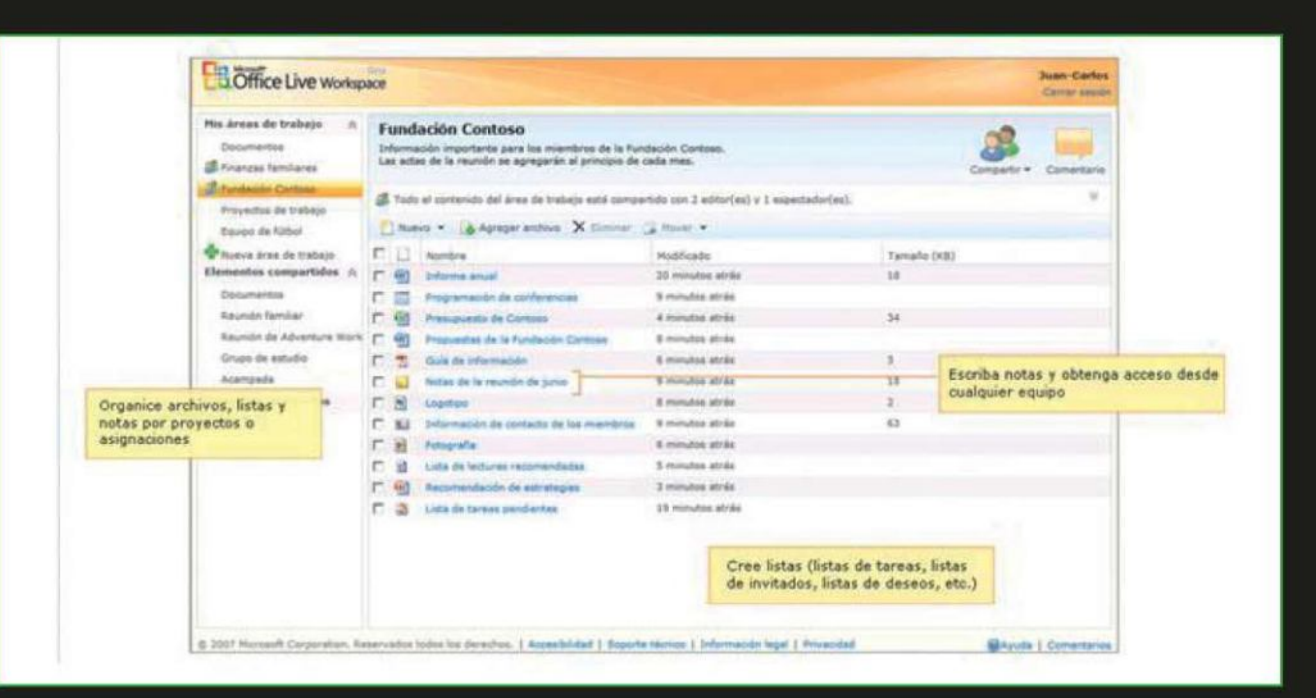
>>> TAMBIÉN TOMA NOTA DE...

- **Slide Rocket (www.sliderocket.com): Es una alternativa bastante interesante al clásico programa de presentaciones Powerpoint de Microsoft. Te permite tener estas presentaciones colgadas en la Web o publicarlas a través de las ya populares redes sociales.**
- **Lotus Sametine Unyte (www.unyte.net): Es una aplicación de escritorio que cuenta con el respaldo de IBM. El servicio que es gratuito tiene el inconveniente de que los usuarios sólo pueden colaborar uno a uno. Para subsanar este inconveniente y que varias personas de manera simultánea visualicen nuestro escritorio, compartan documentos y tengan acceso al control de la función llamada escritorio remoto se exige inscribirse en uno de sus planes de suscripción.**
- **Dabbleboard (www.dabbleboard.com): Una original pizarra colaborativa virtual sencilla de utilizar y que incorpora funciones de chat de vídeo y de voz. Es muy útil para compatir dibujos con otros usuarios públicamente.**
- **Etherpad (www.etherpad.com): Se trata de un bloc de notas colaborativo virtual que admite la edición simultánea y el seguimiento de los cambios que se hacen. Tiene la ventaja de que puede guardar el historial de todas las revisiones por lo que se facilita la revisión de las versiones anteriores**

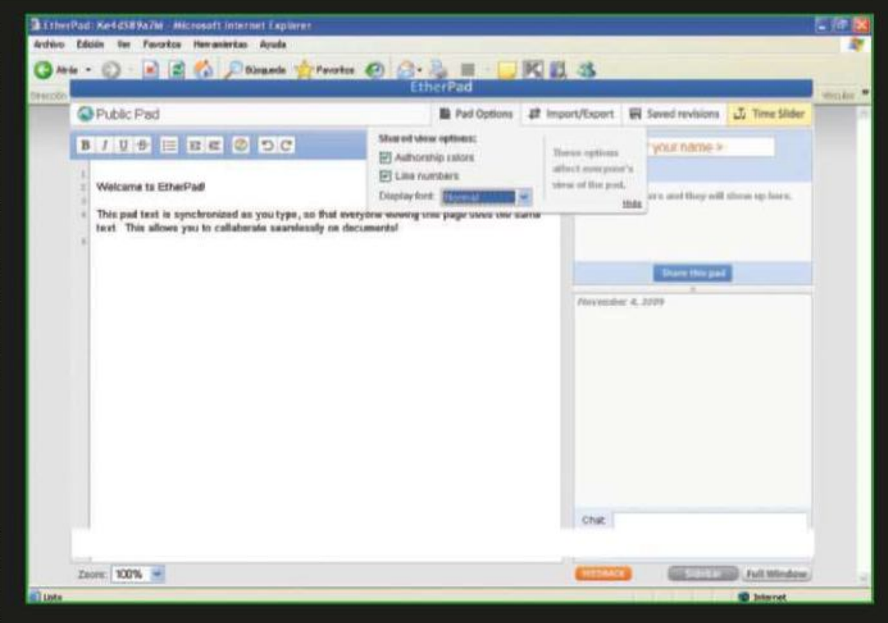








Merece la pena detenerse unos instantes en la aplicación Sheet para las hojas de trabajo. Cuenta con diversas fórmulas clasificadas por categorías y un repertorio bastante diversificado de herramientas para crear gráficos. Además, el usuario tiene la opción de crear macros que mejoran y agilizan los procesos de trabajo. En el caso de Zoho Presentations, se tiene acceso a una vista normal de trabajo, vista de organizador y vista miniaturas. También propone una ventana para notas muy cómoda y útil.



Otras alternativas

Esta fiebre por la nube informática cada vez va más en aumento, de modo que los internautas tienen mayores alternativas entre las que elegir. Aunque Google Docs y Zoho sean quizás las herramientas más conocidas, en el universo web es posible encontrar otras soluciones. Este es el caso de Adobe: desde la página www.acrobat.com es posible utilizar vía web su procesador de textos Buzzword, convertir archivos PDF vía on-line y almacenar y compartir documentos de una manera también sencilla y rápida.

Por su parte, y con un carácter más específico, los amantes de la edición de vídeo tienen la posibilidad de emplear Pinnacle Share (www.pinnaclesys.com), pensado sobre todo para las personas que previamente han editado sus vídeos con algunos de los programas de escritorio de esta conocida firma. Y para los amantes de la fotografía las opciones principales son dos: Photoshop Express (www.photoshop.com) y Picnick (www.picnik.com).

Con ellas básicamente se proporcionan herramientas encaminadas a realizar retoques bastante sencillos de las imágenes que los internautas difunden a través de la Internet. A este listado hay que sumar también el programa Splashup (www.splashup.com) que se asemeja a los editores gráficos de escritorio y que permite trabajar con capas y Concept Share (www.conceptshare.com). Esta herramienta tiene un perfil más profesional y puede utilizarse de manera gratuita durante un período de un mes. Es muy útil para aquellos usuarios que, por su trabajo, necesitan compartir bocetos gráficos.

Wii Fit Plus

Combate el estrés y el sedentarismo

El juego más vendido de 2008 y 2009 se actualiza con el mismo objetivo: conseguir que el español medio se ponga en forma mientras se divierte. Wii Fit Plus es la versión avanzada de este peculiar entrenador personal que, en esta ocasión, incluye novedades que tratan de responder a las necesidades de los jugadores del Wii Fit original. Para ello, permite personalizar aun más los ejercicios con el fin de evitar los "azotes" más comunes que nos acechan: el estrés, los dolores de espalda, el sedentarismo y la mala alimentación.

Para lograrlo, Wii Fit Plus propone 15 nuevas actividades, como el yoga y la tonificación. También existe la opción de crear tablas personalizadas de los ejercicios. Y es que está demostrado que el ejercicio físico que se practica de forma regular contribuye a rebajar los estados de estrés y ansiedad y, además, ayuda a que mejoremos nuestra imagen corporal y que nuestro organismo produzca endorfinas con efecto euforizante para sentirnos muchos mejor. Tal y como señala Reyes Ramírez, doctora en Medicina especializada en medicina familiar y comunitaria: "Wii Fit Plus, sin que sea un





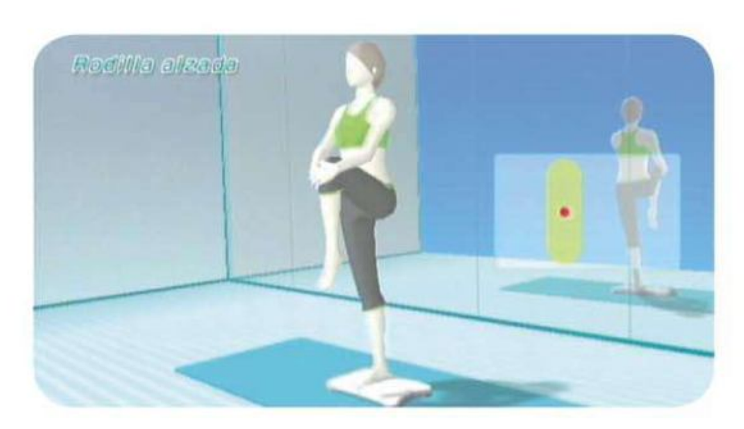






sustituto de la ayuda profesional, puede ser un complemento interesante". Por otro lado, la edición revisada del popular juego de Nintendo permite que tengamos un control del gasto de calorías que conseguimos con el ejercicio, lo que resulta una excelente fórmula y alternativa para evitar coger algún que otro kilo de más. Y es que el juego nos ayuda a saber no sólo las calorías que ingerimos, sino también de las que gastamos. Wii Fit Plus también nos ayuda a combatir el sedentarismo ya que disfraza el deporte que hacemos a través del juego, y permite marcarse objetivos y comparar con otros jugadores los logros que alcanzamos.

Tiene un divertido modo multijugador destinado al entrenamiento en compañía de la familia y los amigos.

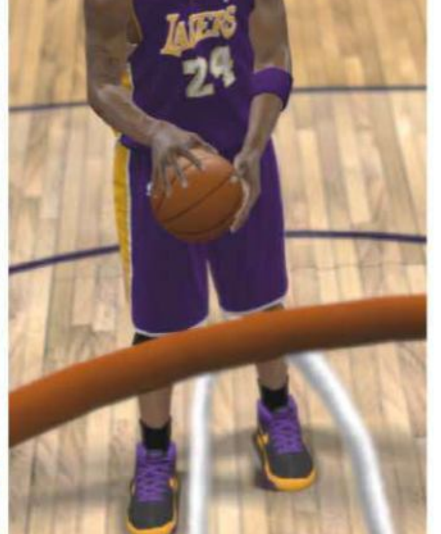




La mejor liga de baloncesto del mundo









Pau Gasol, Kobe Bryant, Carmelo Anthony o Yao Ming. Todos ellos tienen en común una cosa: juegan en la NBA, la mejor liga de baloncesto en la que el buen juego y el espectáculo siempre están garantizados. Sus seguidores están de enhorabuena porque ya tienen la oportunidad de disfrutar del videojuego de la NBA por excelencia que este año celebra su décimo cumpleaños. Disponible para PC y las consolas Wii de Nintendo, Xbox 360 de Microsoft y la PS2 y Playstation 3 de Sony, sus gráficos proporcionan una excelente experiencia de juego que resulta muy real; tanto es así que se tiene la sensación de estar ante un partido de los de verdad. Los controles ahora son mucho más intuitivos y fáciles de utilizar, una característica que permite que efectuemos movimientos (tanto ofensivos como defensivos) que contrarresten las acciones del rival y decidamos cómo defender los tiros a canasta. 2K10 incorpora el modo "NBA hoy" para no perder detalle de todo cuanto acontece en la liga NBA de verdad: noticias, estadísticas, enfrentamientos, etcétera. Asimismo, el informador de 2K y su equipo de analistas proporcionan información de los jugadores y sus equipos. Estos datos están actualizados constantemente y se recogen valoraciones de los jugadores, lesiones y traspasos. También se ha incluido un modo de juego on-line.









El regreso de El Torneo del Puño de Hierro

Han tenido que pasar cuatro años para que se pusiera a la venta un nuevo videojuego de la saga Tekken, pero la espera ha merecido la pena. El Torneo del Puño se Hierro ha vuelto con más fuerza de nunca y su incursión, por primera vez, en las plataformas Xbox 360 y Playstation 3 promete, y mucho, para los fieles a los títulos de lucha.

La trama gira en torno a la batalla por el control del imperio de la familia Mishima. Se han incluido 42 personajes, muchos de ellos caras conocidas y otras nuevas como la del primer español que participa en este encuentro: Miguel Caballero. Pero este guiño a nuestro país no es el único, pues uno de los nuevos escenarios de este Tekken 6 está inspirado en la ya popular (e internacional) Tomatina de Buñol. Con gráficos en Alta Definición, es posible participar en luchas on-line y optar a un combate que se llama modo Campaña, uno de los alicientes más destacados de este juego: se propone un sistema de control mixto en el que se combina la libertad de movimientos y el empleo de armas con el sistema de lucha tradicional al que Tekken nos tiene acostumbrados.









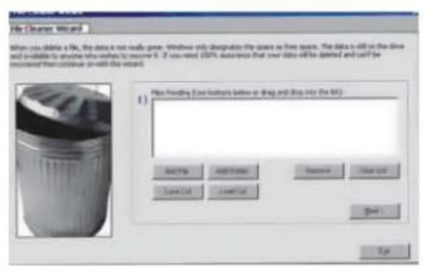


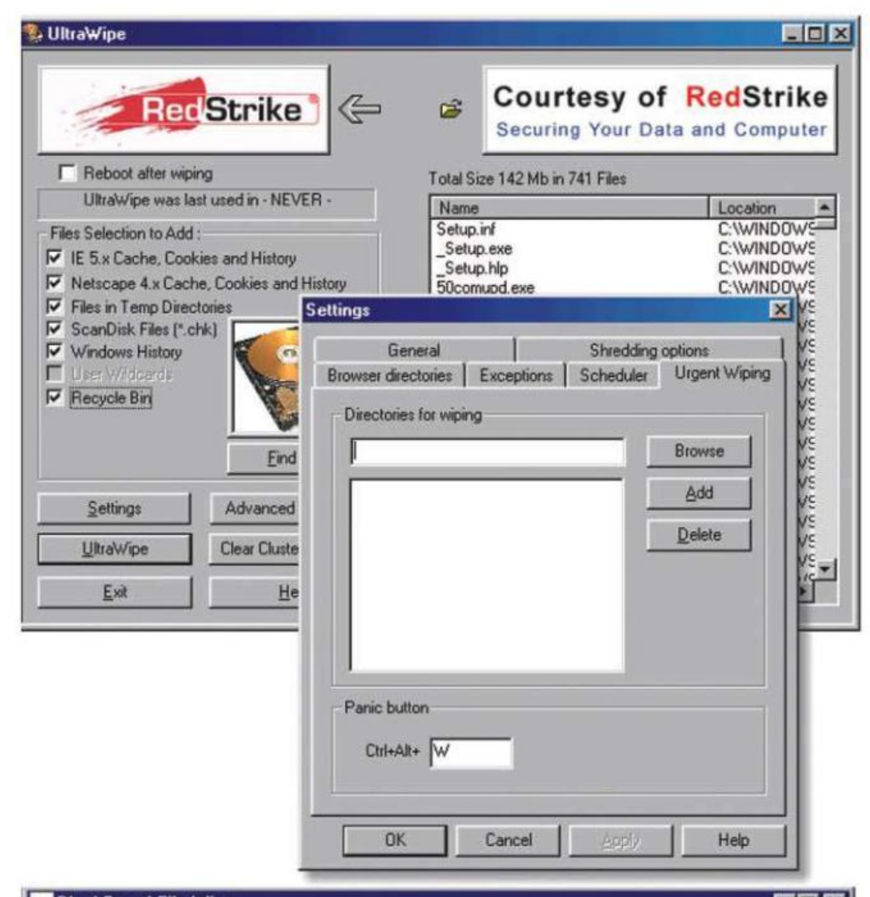


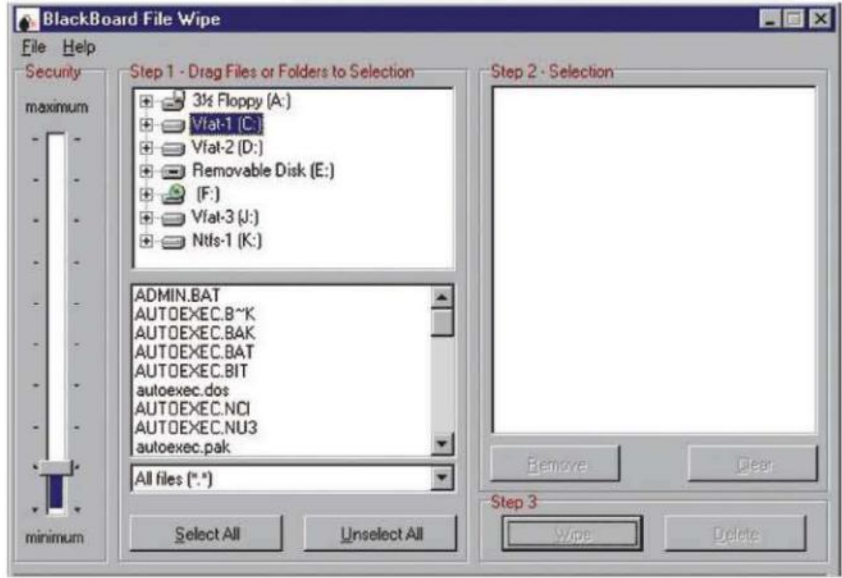


¿Cómo borrar realmente un archivo del ordenador?

La mayoría de la gente sabe que en un sistema Windows se puede recuperar un archivo una vez se ha enviado a la papelera de reciclaje. Lo que casi todos desconocen es que, una vez vaciada la papelera, el fichero aun no ha sido perdido para siempre. Y es que al eliminarlo, no desaparece físicamente sino que sólo se consigue que el sistema operativo no lo muestre más. La información que contiene sigue existiendo, y permanece magnetizada en los clusters del disco duro. ¿En que momento se borra entonces? Únicamente cuando el espacio que ocupa se sobrescribe posteriormente por otro archivo. Pero que no cunda el pánico: existen varias herramientas que permiten borrar los ficheros cambiando los bytes de los clusters por valores "00". Existen en la red varios programas gratuitos dirigidos a ello. Uno es Sure Delete, que se encarga de eliminar por completo los archivos que se desee. BlackBoard FileWipe hace posible, a su vez, borrar cualquier documento sobrescribiéndolo diez veces con datos al azar y después, borrándolo. Por último, UltraWipe se configura para eliminar archivos de tipo común como son los temporales, la memoria caché del navegador, las cookies, el historial de direcciones Web, etc. Para valorar la importancia con la que cuentan estos programas, nada mejor que remitirnos a un estudio realizado recientemente en el Instituto de Tecnología de Massachusetts para el que se reunieron 158 discos duros de diversos lugares. Se obtuvo un dato elocuente: 69 de ellos contenían ficheros recuperables y 40 información crítica que incluía, entre otros datos, los pasos de las transacciones realizadas durante un año en las cuentas de un banco. Y es que no importa cuantas veces se formatee el disco: herramientas como GetDataBack pueden recuperarlos.



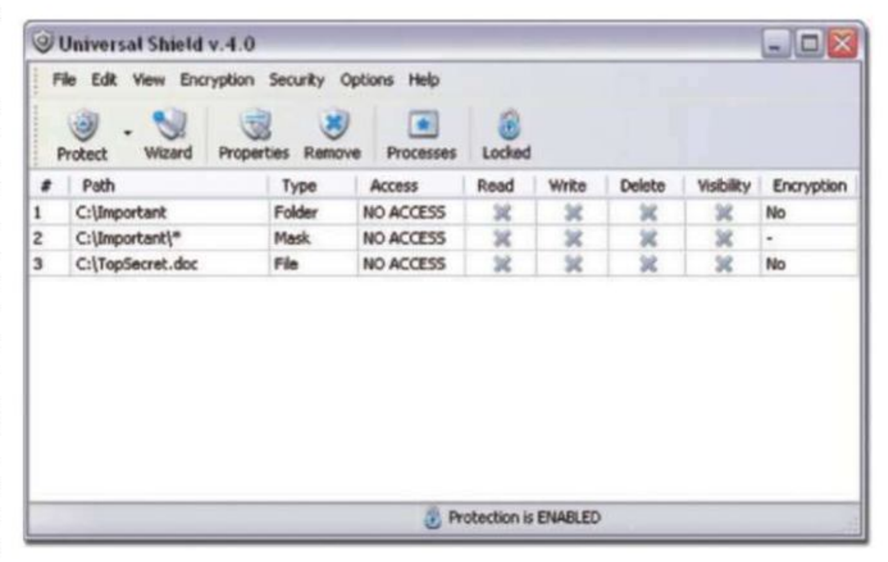




Ocultar, encriptar y proteger carpetas importantes

¿Harto de que te cotilleen las carpetas confidenciales? Como hay fotos, vídeos o documentos que uno no desea compartir con nadie, nada mejor que saber cómo ocultar una carpeta en el PC sin correr el riesgo de que alguien pueda acceder a ella.

Existe un método cómodo y eficaz para hacerlo y que, además, es gratuito. Basta con descargarse el programa Universal Shield. Su manejo es muy fácil para cualquier usuario ya que incluye un asistente que le va guiando paso a paso. Además, hace posible no sólo ocultar carpetas y unidades, sino también encriptar ficheros, marcar ciertos documentos como archivos de sólo lectura o, si se cuenta con la categoría de administrador, hacer uso de algunos pequeños trucos de seguridad que permiten limitar el acceso de otros usuarios a las opciones de configuración del sistema. Una vez se ejecuta Universal Shield, los ficheros ocultos no aparecen en el Explorador de Windows y quedan protegidos también del acceso a través de red local o de Internet. Posibilita también asignar combinaciones de teclas a las carpetas protegidas para, de este modo, acceder a las mismas sin necesidad de ejecutar el programa.



¿Qué hacer si se es víctima del phishing?

Cuando se recibe un intento de ataque phising no debe dejarse pasar. Es importante actuar con celeridad: si se trata de un correo electrónico procedente de una entidad bancaria o similar, no hay duda: se trata de una estafa. Los bancos nunca se ponen en contacto con sus clientes a través de mail, sino que lo hacen siempre vía telefónica. Para que no vuelva a repetirse, conviene seguir estos consejos:

• Ponerse en contacto inmediatamente con el banco o caja de ahorros y explicarles lo que ha ocurrido. En le caso de haber picado en la trampa del estafador, en posible que sea necesario anular la tarjeta o bloquear la cuenta inmediatamente.

• En el caso de que no fuera un banco sino una tienda on-line o similares, se debe informar inmediatamente también del hecho.

• También puede denunciarse al GDT (Grupo de Delitos Telemáticos) de la guardia civil. Esta organización se dedica a combatir todos los delitos y estafas que tienen lugar en la Red.

• Finalmente, para asegurarse de que no vuelva a ocurrir, se puede cambiar las contraseñas de Internet y utilizar otras claves que resulten más complicadas de descifrar.



Zona móviles

REAL FOOTBALL 2010

Los adictos al fútbol ya pueden disfrutar un año más de la pasión de los mejores estadios y la tensión de los derbys más importantes del mundo. Real Football 2010 permite elegir un equipo de entre los 245 que hay disponibles procedentes de ocho ligas con el único objetivo de llevarlo a la gloria. Y no sólo es posible hacerle ganar títulos. También está el tema de los fichajes. ¿Te imaginas a Messi vistiendo la camiseta madridista o a Raul jugando en el Atlético de Madrid? Real Football 2010 también ofrece un modo de juego que se llama leyenda y que nos permite jugar un partido con nuestra estrella favorita. Finalmente, existe la opción de enfrentarse a otros rivales online mediante Bluetooth. El balón ya ha empezado a rodar.









CHUCK NORRIS

Cuando matas a Chuck Norris, Chuck Norris no muere, simplemente se enfada más. Para vivir una aventura con uno de los grandes mitos del cine de acción de todos los tiempos, nada mejor que disfrutar de esta aplicación para el iPhone en la que el usuario podrá descargarse de todas las tensiones de un duro día laboral pegando puñetazos, cabezazos y patadas voladoras a cuantos enemigos se atreva a enfrentarse. Tiene trece niveles de juegos que se desarrollan en tres escenarios diferentes: una jungla asiática, un rancho tejano y las calles de Nueva York. Con la cámara del iPhone podemos sacar fotografías de nuestros amigos y familiares y luego ponerlas en el cuerpo de alguno de los enemigos del protagonista. Una manera sana de ajustar cuentas.









ASTÉRIX Y CLEOPATRA



Coincidiendo con el 50 aniversario del nacimiento de los cómics de Asterix y Obelix, los héroes galos que han seducido a varias generaciones, Gameloft lanza para el móvil este juego que se inspira en una de las aventuras más famosas de la célebre pareja. En ella, la reina Cleopatra, tratando de convencer a Julio César de que la civilización egipcia es superior a la romana, ordena la construcción de un fastuoso templo en menos de tres meses. Para ello contrata al famoso arquitecto Edifis, quien contará con la ayuda de Asterix y Obelix. En el caso de no cumplir con el plazo estipulado, el arquitecto será arrojado a los cocodrilos. En este título, el jugador tiene que elegir entre uno de sus dos héroes sin olvidar que, al igual que en los tebeos, ambos lucharán siempre codo con codo. Los gráficos ayudan a sumergirse en las aventuras y pelear contra los enemigos. ¿Te atreves a unir las piezas que forman la inmensa obra de Cleopatra?



